IP PBX SC-32

Guía de Administrador

Versión 70.19.56.34

Tabla de Contenidos

1. Introducción 5
1.1 Funcionalidades 5
1.2 Especificaiones de Hardware 6
2. Configuración del Sistema 8
2.1 Plano de Conexión 8
2.2 Conexión de Cable Ethernet 8
2.3 Fuente de Alimentación 8
3. Administrador Login 10
4. Estados 13
4,1 Estados de Linea 13
4.1.1 Estados de Extensión 13
4.1.2 Estados de Troncal 13
4,2 Estados del Sistema 14
4.2.1 Info del Sistema 14
4.2.2 Estados de Red 15
5. Sistema 15
5.1 Preferencias de Red 15
5.1.1 Configuraciones de LAN 16
5.1.2 Servidor DHCP 17
5.1.3 Configuraciones de VLAN 17
5.1.4 Configuraciones de VPN 19
5.1.5 Configuraciones de DDNS 20
5.1.6 Route Estático 21
5.2 Configuraciones de Seguridad 22
5.2.1 Centro de Seguridad 22
5.2.2 Firewall Rules 23
5.2.3 Lista Negra de IP 26
5.2.4 Configuraciones de AMI 27
5.2.5 Donación de Database 28
5.2.6 Configuraciones de Alerta 29
5.3 Servidor LDAP 31
5.3.1 Servidor LDAP 31
5.4 Administración de Almacenamiento 33
5.4.1 Almacenamiento Externo 33
5.5 Preferencias del Sistema 35
5.5.1 Configuraciones de Contraseña 36
5.5.2 Fecha y Tiempo 37
5.5.3 Actualización de Firmware 38
5.5.4 Copia de Seguridad y Restaurar 39
5.5.5 Restablecer y Reiniciar 40
6. PBX 41

6.1 Extensiones 41
6.1.1 Extensiones FXS/VoIP 41
6.1.2 Aprosionamiento de Teléfono 52
6.2 Troncales 60
6.2.1 Troncal Físico 60
6.2.2 Troncal VoIP 68
6.3 Control de Llamada Saliente 78
6.3.1 Routes Salientes 78
6.3.2 Configuraciones de Marcado Rápido 80
6.4 Control de Llamada Entrante 81
6.4.1 IVR 81
6.4.2 Grupo de Timbre 84
6.4.3 Cola 86
6.4.4 Conferencias 89
6.4.5 Routes Entrante 90
6.5 Configuraciones de Audio 95
6.5.1 Audios Personalizados 95
6.5.2 Audios de Música en Espera 97
6.5.3 Configraciones de Audios del Sistema 98
6.6 Configuraciones Básicas 98
6.6.1 Preferencias Generales 98
6.6.2 Horarios de Negocios 101
6.6.3 Códigos de Funciones 103
6.6.4 Configuraciones de Voicemail 106
6.7 Configuraciones Avanzada 110
6.7.1 Configuraciones de SIP 110
6.7.2 Configuraciones de IAX 118
6.7.3 Lista Negra 119
6.7.4 Configuraciones de Callback 120
6.7.5 Configuraciones de DNIS 122
6.7.6 DISA 122
6.7.5 Configuraciones de PIN Usuario 123
6.7.8 Configuraciones de PIN 125
6.7.9 Grupos de Paging 126
6.7.10 Certificados 127
7. Reportes 128
7.1 Registros de Llamada 128
7.2 Registros de Sistema 129
8. Logout 130
9. Use UNI-K 130
9.1 Hacer Llamadas Salientes 130
Ejemplo de Enrutamiento vía Troncal VoIP 131
9.2 Llamada Entrante 134

Ejemplo de Enrutamiento a un IVR 134
APPENDIX A FAQ 136
APPENDIX B ¿Cómo configura Almacenamiento Externo? 137
APPENDIX C ¿Cómo Configura NAT? 139
APPENDIX D ¿Cómo Utiliza Auto Provisión? 141
APPENDIX E ¿Cómo Puedo Configurar los Tonos Distintivos? 144
APPENDIX F Cómo utiliza DID 146
APPENDIX G ¿Cómo utiliza Tecla BLF a Seleccionar Línea PSTN? 150
APPENDIX H Guía de Configuración de Seguridad de UNI-K 151
APPENDIX I Cómo Utiliza TLS en UNI-K 177
I.1 Cómo registra teléfonos IP a UNI-K vía TLS 177
I.2 Cómo registra troncal SIP al proveedor VoIP vía TLS 201
APPENDIX J ¿Cómo Utiliza LDAP? 203

1. Introducción

UNI-K IP PBX SC-32—IP-PBX para Negocios

Medianos/Oficina IP PBX SC-32

UNI-K IP PBX SC-32 es una PBX independiente incorporada e híbrida para empresas medianas y oficinas sucursales remotas de organizaciones grandes. UNI-K también ofrecen una solución híbrida (una combinación de aplicaciones de VoIP utilizando equipamiento telefónico tradicional) alternativa para las Enterprises que aún no están listos para migrar a una solución VoIP completa.

***Nota: Esta guía se aplica a UNI-K IP PBX SC-32 V4, las imágenes de hardware en este documento son UNI-K IP PBX SC-32 V4.**

1.1 Funcionalidades

• Alerta	• Follow me
• Auto-provisión	• HTTPS
• Lista Negra	• Herramientas incorporada de captura de paquetes integrada
• BLF Soportada	• Respuesta Interactiva de Voz (IVR)
• Transferencia Ciega	• Intercom/Zone Intercom
• Call Back	• L2TP
• Registros Detallados de Llamadas (CDR)	• LDAP
• desvío de Llamadas	• Extensión Móvil
• Llamadas Paradas	• Administradores Múltiples
• Llamadas Pickup	• Música en Espera
• Grabación de Llamadas	• Música en Transferencia
• Ruteo de Llamadas	• Open VPN
• Transferencia de Llamadas	• Paging/Zone Paging
• Transferencia de Llamadas	• PIN Usuarios
• Llamadas en Espera	• QoS
• ID del Llamador	• Cola de Llamadas
• Conferencia	• Grupo de Timbre
• Data base Grant	• Ruteo por ID de Llamador
• DDNS	• Centro de Seguridad
• Definir Horario Oficial	• Skype Integración (Skype Connect)
• Marcar por Nombre	• Marcación Rápida

• DIDs	• Funciones monitoreo
• Acceso Directo al Sistema Interno (DISA)	• Ruteo Estático
• Tono Distintivo	• T.38
• No Moleta(DND)	• Llamada Tripartita
• Almacenamiento Externo	• VLAN
• Firewalls	• Voicemail

Para más información, por favor haga clic:
http://www.unik-latam.com

1.2 Especificaciones de Hardware

1) Panel Frontal

Figura 1-1 UNI-K IP PBX SC-32 Panel Frontal

No.	Identificación
①	LED Verde indica la conexión de energía es normal.
②	LED verde indica el sistema del servidor está funcionando en orden.
③	LED Verde indica el sistema está preparado.
④	LED verde indica el interfaz de Internet está en uso.
⑤	LED rojo se refiere al puerto FXO LED naranja indica presencia de un puerto BRI. LED verde se refiere al puerto FXS LED Rojo parpadeado: El puerto FXO no está conectado con la PSTN línea.

	Alternativamente parpadea Rojo y Verde: Puerto FXO tiene una llamada entrante. Alternativamente parpadea Rojo y Verde rápidamente: Puerto FXO está en una llamada. Alternativamente parpadea Verde y Rojo: Puerto FXS está sonando. Alternativamente parpadea Verde y Rojo rápidamente: Puerto FXS está en una llamada.

2) Panel Trasero

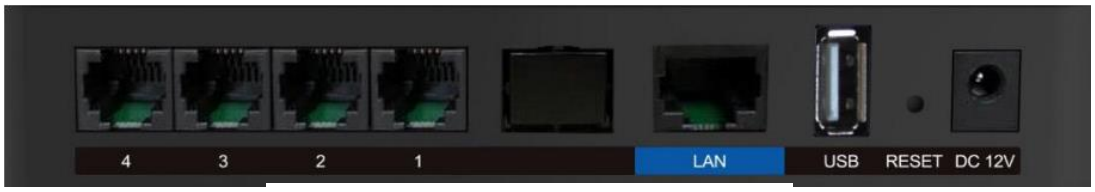


Figura 1-2 Foto de Panel Trasero de

2. Configuración del Sistema

2.1 Plano de Conexión

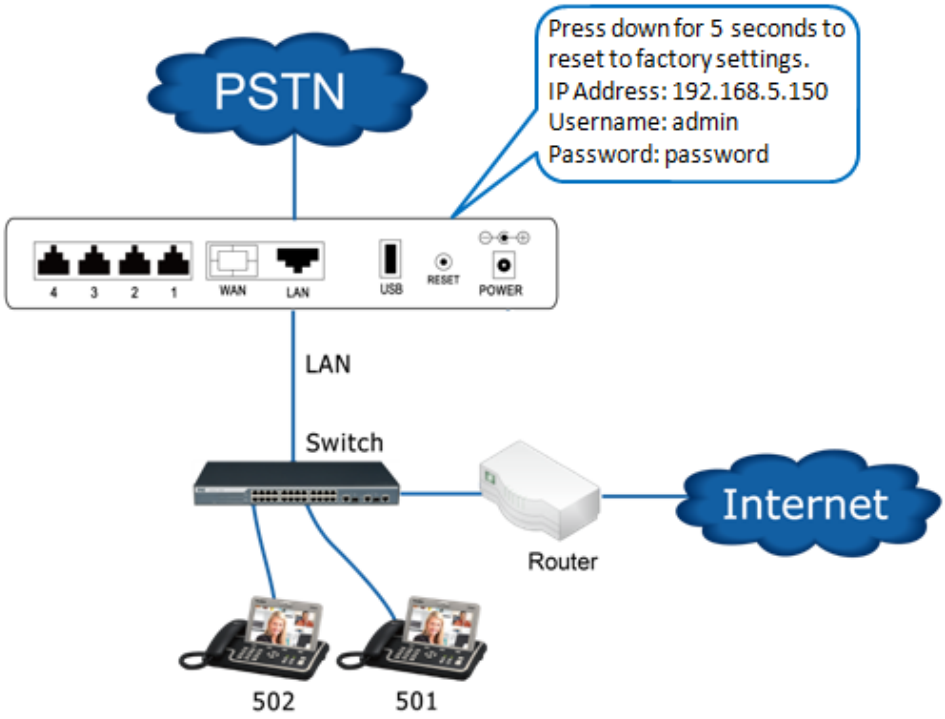


Figura 2-1

2.2 Conexión de Cable Ethernet

UNI-K provee dos puertos de 10/100M Ethernet con interface RJ45 e Indicador LED. Conecte el cable Ethernet al puerto Ethernet del UNI-K, y luego conecte el otro extremo del cable Ethernet con un hub, switch, router, LAN o WAN. Una vez conectada, compruebe el estado del indicador LED. Un LED amarillo indica que el puerto está en el proceso de conexión, y un LED verde indica que el puerto está conectado correctamente.

2.3 Fuente de Alimentación

UNI-K utiliza la fuente de alimentación del interruptor de alto rendimiento, que suministra la potencia necesaria para la unidad.

AC Entrante: 100~240V
DC Saliente: 12V, 1A

Por favor, siga los pasos siguientes para conectar la unidad UNI-K a una toma de corriente:

1. Conecte el extremo pequeño del cable de alimentación al puerto entrante de alimentación del panel dorso de UNI-K, y conecte el otro extremo del cable en una toma de corriente de 100VAC.
2. Revise LED de Energía en el panel frontal. Un LED verde solido indica que se está suministrando energía correctamente.

3. Administrador Login

Desde el navegador, introduzca la dirección IP del servidor UNI-K.
Si esta es la primera vez que está configurando UNI-K, por favor utilice la configuración predeterminada de la manera siguiente (su PC debe estar en la misma red local con UNI-K):
Dirección IP: http://192.168.5.150
Nombre de Usuario: administrador
Contraseña: password
En este ejemplo, la dirección IP es 192.168.5.143

Figura 3-1

Esta es la página de bienvenida de UNI-K IP PBX SC-32 después de inicio de sesión correcto.

Figura 3-2

Usted pueda también iniciar sesión por vía HTTPS protocolo

Como https://192.168.5.147, usted verá un mensaje que es un problema de certificado. Haga clic en "Continue to...", a continuación, puede iniciar sesión después de ingresar usuario y contraseña. HTTPS es HTTP mediante SSL, y es más seguro que HTTP.

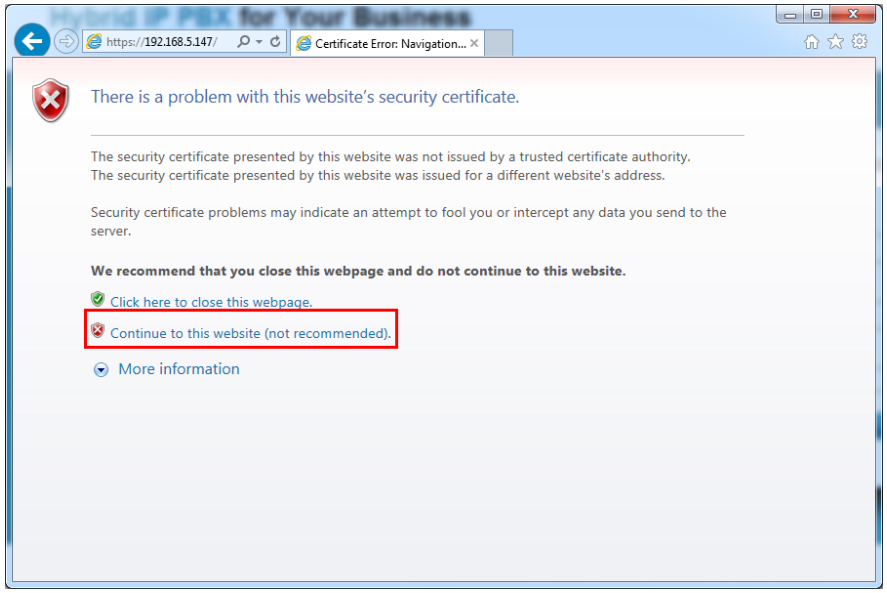

https://192.168.5.147/
Certificate Error: Navigation...
There is a problem with this website's security certificate.
The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).
More information

Figura 3-3

Nota:

UNI-K seguimiento de actualización del firmware

▪ Reinicie el dispositivo dos veces para hacer el firmware nuevo toma efecto.

▪ Elimine el caché y las cookies del navegador antes de iniciar sesión.

▪ Hay un problema de compatibilidad con IE11. Configure "Compatibility View Settings" de navegador IE11, agregue la dirección IP de UNI-K, y comprobar "Display Intranet sites in Compatibility View" y "Use Microsoft Compatibility lists".

Vea la foto siguiente. UNI-K IP es 192.168.5.147 en este ejemplo.

Figura 3-4

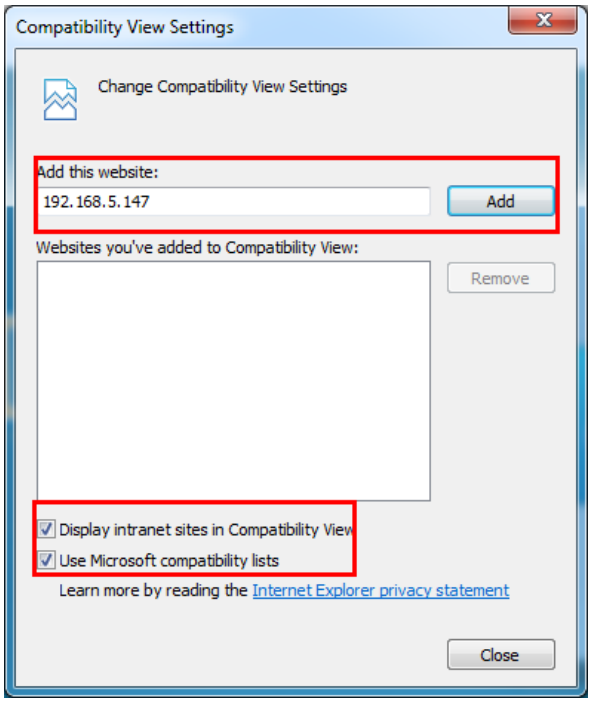


Figura 3-5

4. Estados

Haga clic en

para empezar a revisar los estados de UNI-K IP PBX SC-32. Podemos revisar los estados de las extensiones, troncales, y red y la información del sistema.

4.1 Estados de Línea

En esta página, podemos revisar estados de extensiones y troncales

4.1.1 Estados de Extensión

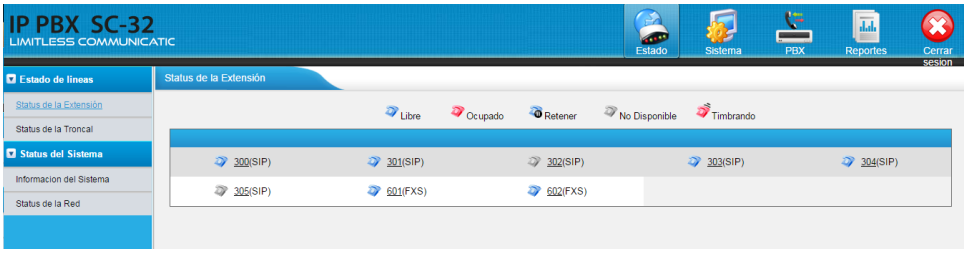


Figura 4-1

Descripción de Estados de UNI-K:

Extensiones:

1) : Extensión no está disponible

2) : Extensión está inactiva

3) : Extensión está sonando

4) : Extensión está ocupada

5) : Extensión está retenida

4.1.2 Estados de Troncal

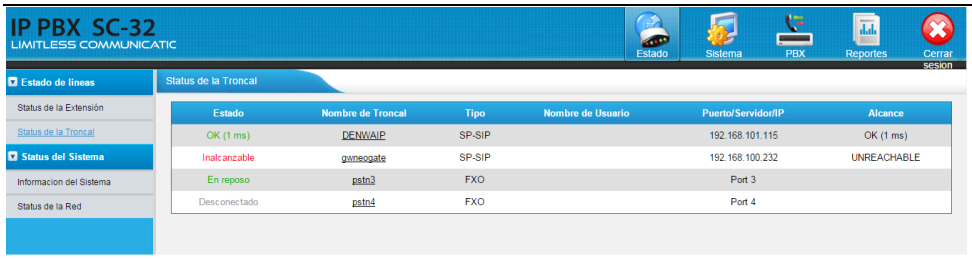


Figura 4-2

Troncales

VoIP Troncal:

Estados

No Registrado: La registración de troncal falló.

Registrado: Registro con éxito, el troncal está listo para su uso.

Enviar Solicitud: Registrando.

Esperando: Esperando por la autenticación.

Proveedor de Servicio:

Estados

OK: Registro con éxito, el troncal está listo para su uso.

Inaccesible: El troncal es inaccesible.

Fallado: La registración de troncal falló.

FXO Troncal:

Estados

Inactivo: El puerto es inactivo.

Ocupado: El puerto está en uso.

Desconectado: El puerto no está conectado con la PSTN línea.

Más detalles, por favor refiérase al indicador LED del panel frontal.

Troncal BRI:

Estados

Ok: Los puertos están conectados correctamente.

Desconectado: El puerto no está conectado con la BRI línea.

4.2 Estados del Sistema

En esta página, podemos comprobar el estado del sistema UNI-K, incluyendo el hardware, versión de firmware y los estados de la red.

4.2.1 Info del Sistema

En esta página, se puede comprobar la versión de hardware / firmware, o el uso del disco de UNI-K.

Figura 4-3

4.2.2 Estados de Red

En esta página, la dirección IP del puerto LAN aparecerá. Si Open VPN y VLAN fueron configurados bien, la información se aparezca aquí también.

Figura 4-4

5. Sistema

Haga clic en

para accederse.

En esta página, podemos configurar las configuraciones de la red, configuraciones de firewall, administración de almacenamiento y algunas otras configuraciones como actualización de firmware.

5.1 Preferencias de Red

5.1.1 Configuraciones de LAN

Figura 5-1

·DHCP
Si está establecida esta opción, UNI-K utilizará DHCP para obtener una dirección IP disponible en su red local. No se recomienda ya que sin la dirección IP correcta no se puede acceder a UNI-K.

·Habilita SSH
Esta es la forma avanzada para acceder al dispositivo, se puede utilizar el software de masilla para acceder al dispositivo. En el acceso SSH, se puede hacer más configuraciones avanzadas y de depuración, es desactivado por defecto.

·Puerto: Por defecto es 8022; puede cambiarlo.
·Hostname
Establece el host name para UNI-K.

·Dirección IP
Establece la dirección IP para UNI-K.
Es recomendable que una dirección IP estática para UNI-K.

·Subnet Mask
Establece la Subnet Mask para UNI-K.

·Gateway
Establece el gateway para UNI-K.

·Primary DNS
Establece la Primary DNS para UNI-K.

·Secondary DNS
Establece la secondary DNS para UNI-K.

·Dirección2 IP

Establece la segunda dirección IP para UNI-K.

·Subnet Mask2

Establece la segunda Subnet Mask para UNI-K.

5.1.2 Servidor DHCP

Dynamic Host Configuración Protocolo (DHCP) es un protocolo de red que permite a un servidor asignar automáticamente una dirección IP a un computador desde un rango definido de números (es decir, un ámbito de aplicación) configurado para una red dada. También puede establecer una red local de servidor NTP para UNI-K aquí.

Nota: UNI-K IP PBX SC-32 puede trabajar como un DHCP servidor, pero no puede ser considerando como un router.

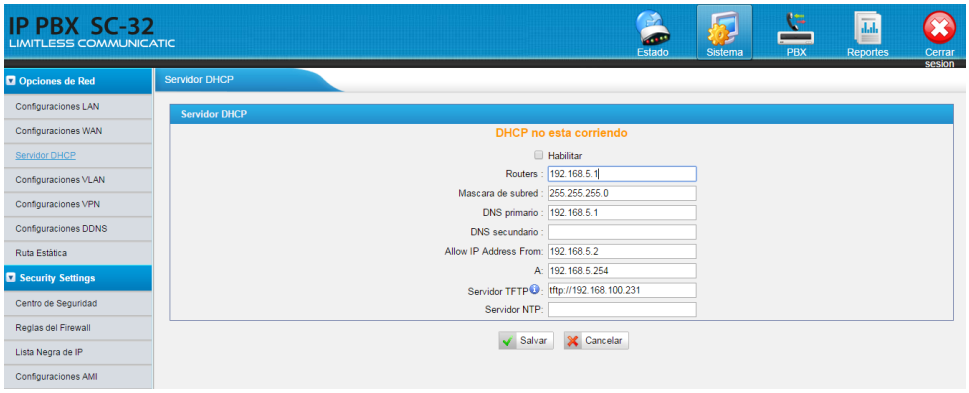


Figura 5-2

5.1.3 Configuraciones de VLAN

Una VLAN (LAN Virtual) es una red lógica de área local (o LAN) que se extiende más allá de una sola LAN tradicional a un grupo de segmentos de LAN, dado configuraciones específicas.

Nota:

UNI-K IP PBX SC-32 no es el servidor VLAN, todavía se necesita un interruptor de 3 capas, configure la información de la VLAN allí primero, y luego ingrese los detalles en UNI-K, por lo que los paquetes a través de UNI-K se añadirán la etiqueta VLAN antes de enviar a ese interruptor.

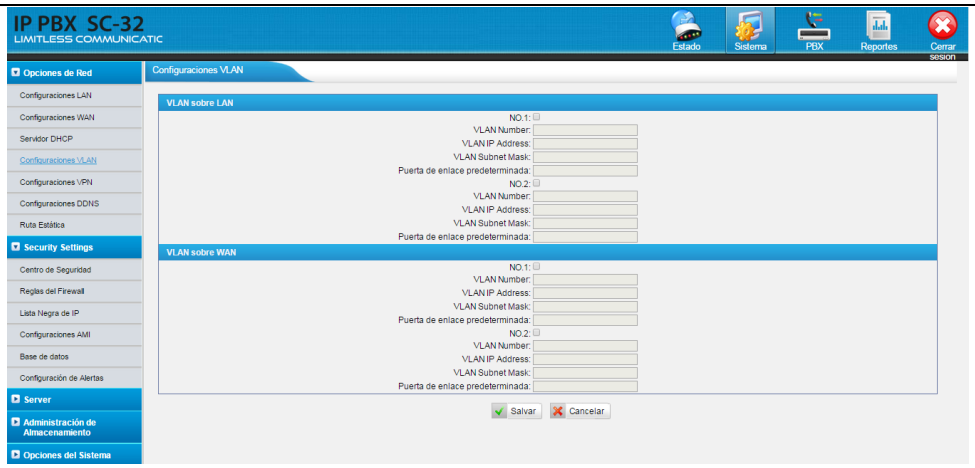


Figura 5-3

VLAN Mediante LAN

·NO.1

Haga clic en NO.1 puede editar el primer VLAN mediante LAN.

·VLAN Número

.El VLAN Número es un valor único que se asigna a cada VLAN en un solo dispositivo.

·Dirección IP de VLAN

Establece la dirección IP para VLAN mediante LAN de UNI-K.

·VLAN de Subnet Mask

Establece Subnet Mask para VLAN mediante LAN de UNI-K.

·Gateway por defecto

Establece gateway por defecto para VLAN mediante LAN de UNI-K.

·NO.2

Haga clic en NO.2 puede editar el primer VLAN mediante LAN.

·VLAN Número

.El VLAN Número es un valor único que se asigna a cada VLAN en un solo dispositivo.

·Dirección IP de VLAN

Establece la dirección IP para VLAN mediante LAN de UNI-K.

·VLAN de Subnet Mask

Establece Subnet Mask para VLAN mediante LAN de UNI-K.

·Gateway por defecto

Establece gateway por defecto para VLAN mediante LAN de UNI-K.

5.1.4 Configuraciones de VPN

Una red virtual privada (VPN) es un método de Redes de computador -típicamente usando internet público - que permite a los usuarios compartir información privada entre ubicaciones remotas, o entre una ubicación remota y una red doméstica de negocios. Una VPN puede proporcionar el transporte seguro de la información mediante la autenticación de usuarios, y el cifrado de datos para evitar que personas no autorizadas puedan leer la información transmitida. La VPN puede ser usada para enviar cualquier tipo de tráfico de red seguramente. UNI-K soporta Open VPN, IPSec y L2TP.

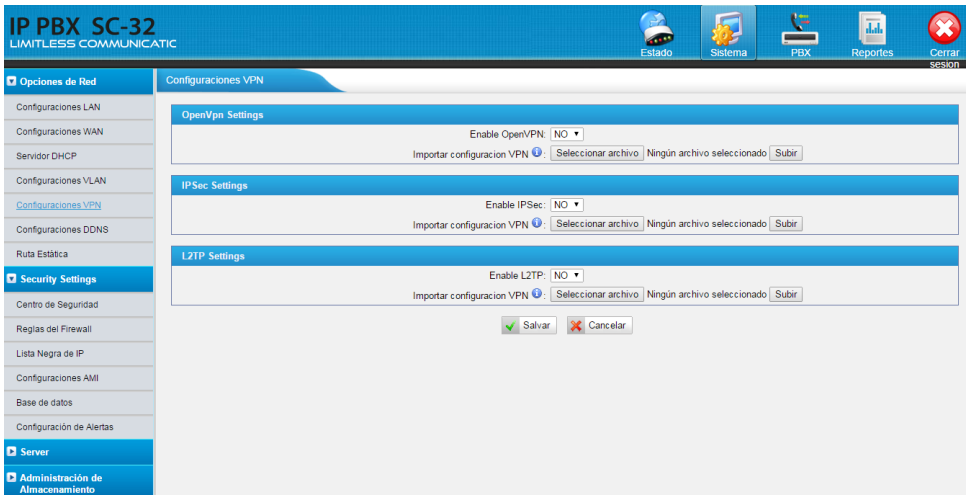


Figura 5-4

·Habilita Open VPN

·Importa VPN Perfil

Importa el archivo de configuración de Open VPN. No configura “user” y “group” en el archivo “config”.

·Habilita IPSec

·Importa VPN Perfil

Importa el archivo de configuración de IPSec. Sólo puede haber una "lan" en el archivo "conf".

·Habilita L2TP

·Importa VPN Perfil

Importa el archivo de configuración de L2TP. Sólo puede haber un "conn" en el archivo "conf".

Nota: para más detalles sobre la configuración VPN anteriores, por favor póngase en contacto con nuestro soporte técnico.

5.1.5 Configuraciones de DDNS

DDNS (DNS Dinámico) es un método / protocolo / red de servicio que proporciona la capacidad para un dispositivo de red, como por ejemplo un sistema de router o computador utilizando el Protocolo de Internet Suite, para notificar a un sistema del servidor de nombres de dominio (DNS) para cambiar, en tiempo real, la configuración DNS activa de sus nombres de host configurados, direcciones u otra información.

Figura 5-5

·Habilita DDNS

·DDNS Servidor

Seleccione el DDNS servidor que se inscribe para el servicio.

·Nombre del Usuario

El nombre del usuario que le proporcione el DDNS servidor.

·Contraseña

Contraseña de la cuenta del usuario.

·Host Name

Nota: DDNS le permite acceder a la red mediante nombres de dominio en lugar

de direcciones IP. El servidor gestiona el cambio de dirección IP y actualiza la información de su dominio de forma dinámica. Debería registrarse para el servidor mediante dyndns.org, freedns.afraid.org, www.no-ip.com, www.zoneedit.com

5.1.6 Route Estático

UNI-K tendrá más de una conexión a Internet en algunas situaciones, pero tiene sólo un gateway predeterminado. Usted tendrá que configurar algunos Route estático para UNI-K a forzarlo para salir por gateways diferentes cuando accede a Internet diferente.
La prioridad del gateway predeterminado de UNI-K de mayor a menor es Open VPN→WAN puerto→LAN puerto.

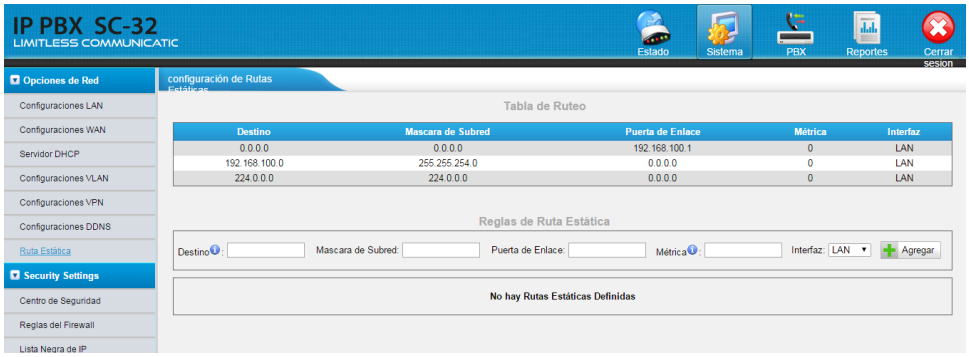


Figura 5-6

1) Tabla de Route
Las reglas de route actual de UNI-K

·Destinación
La destinación de red para ser accedido por UNI-K.

·Subnet Mask
Especifique la destinación de la porción de red.

·Gateway
Definir cuál gateway que UNI-K atravesará cuando accede a la destinación de red.

·Métrico
El costo de un route se calcula utilizando lo que se llama métrica de enrutamiento. Métricas de enrutamiento se asignan a los routes por protocolos de enrutamiento para proporcionar estadística medible que puede ser utilizado

para juzgar lo útil (cómo bajo coste) es un route.

·Interface
Define por cuál internet puerto para pasarse.

2) Reglas de Route Estático
Puede añadir una regla nueva de route estático aquí.

5.2 Configuraciones de Seguridad

Los firewalls se utilizan para evitar que los usuarios de Internet sin autorizaciones tengan acceso a redes privadas que conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del firewall, que examina cada mensaje y bloquea aquellos que no cumplen con los criterios de seguridad especificados.

5.2.1 Centro de Seguridad

Puede chequear la configuración de seguridad de UNI-K en la página "Security Center". Y también, puede ingresar en la página configuración de seguridades pertinentes con rapidez.
Firewall:

Figura 5-7 Centro de Seguridad—Firewall

En la tab de "Firewall", puede chequear la configuración de firewall y configuraciones de alerta. Al hacer clic en el botón correspondiente, puede ingresar en la página de configuración directamente.

Servicio:

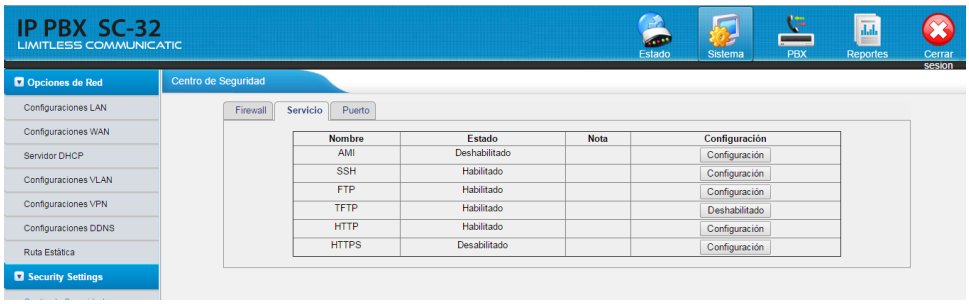


Figura 5-8 Centro de Seguridad—Servicio

En tab de "Servicio", puede chequear estados de AMI/SSH/TFTP. Para AMI / SSH, puede ingresar en la página correspondiente haciendo clic en la botón de la columna "Settings". Para TFTP, puede activar o desactivar directamente.

Puerto:

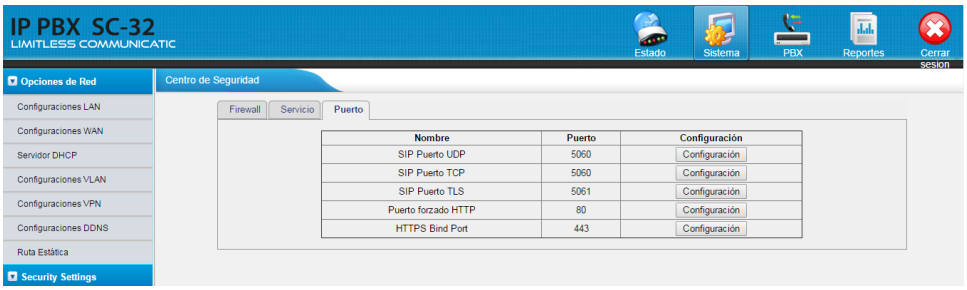


Figura 5-9 Centro de Seguridad—Puerto

En la tab de "Port", puede chequear puerto SIP y puerto HTTP. Puede ingresar también en la página correspondiente haciendo clic en el botón de la columna "Settings".

5.2.2 Firewall Rules

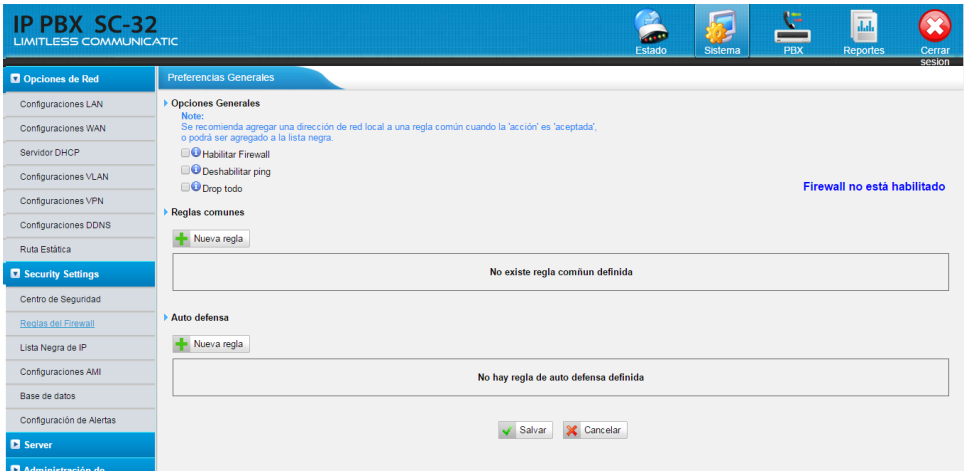


Figura 5-10 Firewall Settings

1) Configuraciones Generales

·Habilita Firewall

Habilita el firewall para proteger el dispositivo.

·Desactiva Ping

Habilitar este artículo, será dado de baja de ping neta de hosts remotos.

·Drop All

En cuando habilita la función de "Drop All", el sistema dará baja todos los paquetes o conexión desde otro hosts si no hay otras reglas definidas. Para evitar el bloqueo de los dispositivos, por lo menos un "TCP" que acepta la regla común, deben ser creados para el puerto utilizado para el acceso SSH, el puerto utilizado para el acceso HTTP y el puerto demandado por el acceso CGI.

2) Reglas Comunes

No hay regla predeterminada; Puede crearlas como requerida.

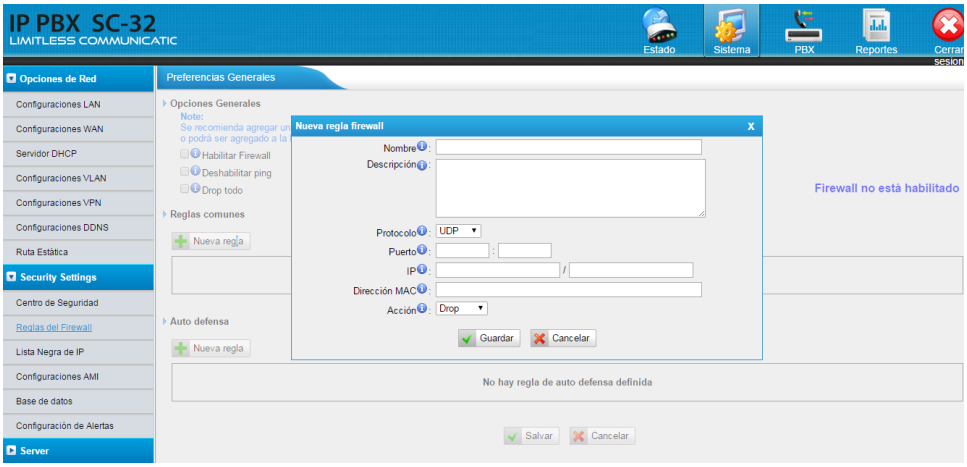


Figura 5-11 Agregan Reglas Comunes

·Nombre

Un nombre para esta regla, por ejemplo "HTTP".

·Descripción

Descripción simple para esta regla. Por ejemplo Acepta host específico para acceder la web interface de configuración.

·Protocolo

Protocolos para esta regla.

·Puerto

Puerto inicial debe estar en el puerto izquierdo y el final debe ser a la derecha. El puerto final debe ser igual o mayor que iniciar puerto.

·IP

La dirección IP para esta regla. El formato de la dirección IP es: IP/mask
Por ejemplo 192.168.5.100/255.255.255.255 para IP 192.168.5.100
Por ejemplo 216.207.245.47/255.255.255.255 para IP 216.207.245.47
Por ejemplo 192.168.5.0/255.255.255.0 para IP desde 192.168.5.0 a 192.168.5.255.

·Dirección MAC

El formato de la dirección MAC es XX:XX:XX:XX:XX:XX, X significan 0~9 o A~F en hex, la A ~ F no diferencian mayúsculas y minúsculas.

Nota: La dirección MAC se puede cambiar cuando es un dispositivo remoto, por lo que no va a trabajar para filtrar el uso de MAC para los dispositivos remotos.

·Acción

Aceptar: Acepta el acceso desde hosts remotos.
Cortar: Corta el acceso desde hosts remotos.
Ignorar: Ignora el acceso.

3) Defensa Automática

Por defecto, no hay la regla.

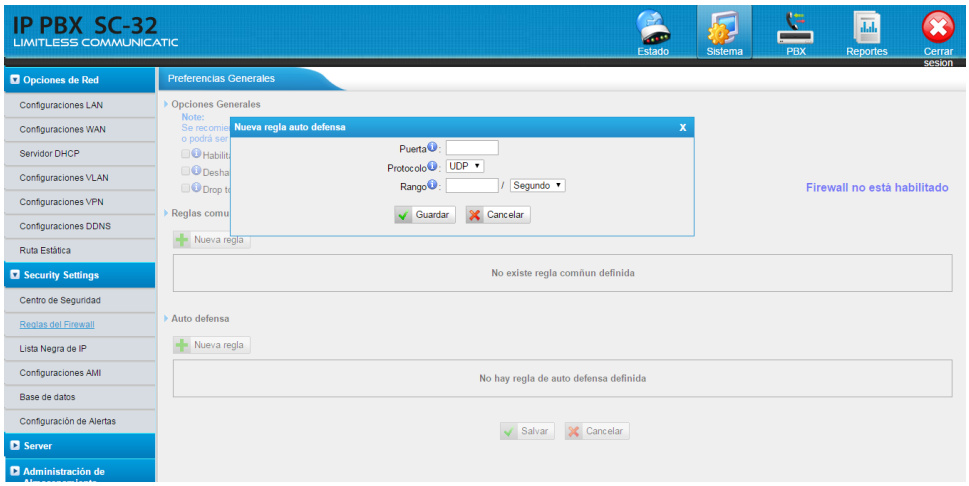


Figura 5-12 Agrega Regla de Defensa Automática

Puerto

El puerto que se requiere defensa automática, por ejemplo, 8022.

Protocolo:

Selecciona el protocolo. Puede seleccionar UDP o TCP.

Tarifa:

Los paquetes o conexiones máximas pueden ser manejados por unidad de tiempo.

Por ejemplo, puede configurarlos como los siguientes:
Puerto: 8022
Protocolo: TCP
Tarifa: 10/min
Entonces, significa conexiones máximas de 10 TCP pueden ser manejados en 1 minuto. La conexión 11 será dado de baja.

5.2.3 Lista Negra de IP

Puede establecer las reglas de la velocidad que acepta los paquetes aquí. Cuando una dirección IP que no haya sido aceptada de las reglas comunes envía los paquetes más rápido que la velocidad permitida, se considerará como dirección IP negra y bloqueará automáticamente.

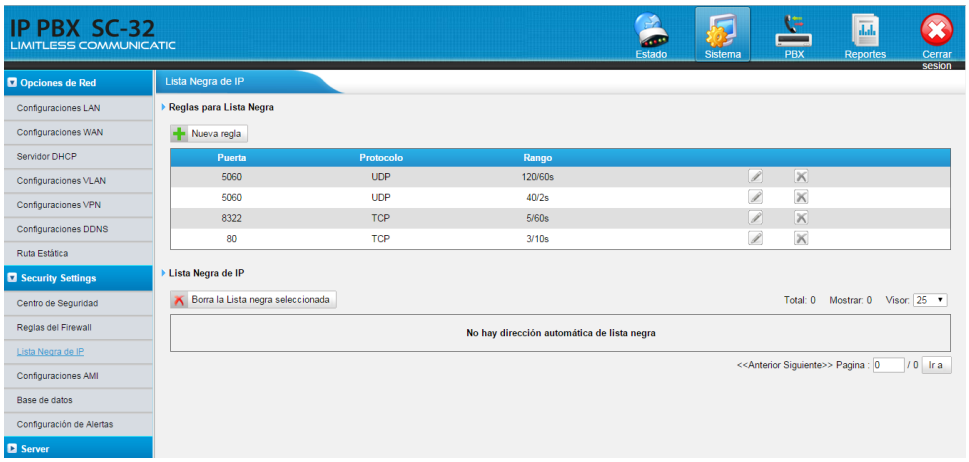


Figura 5-13 Página de Configuraciones de Lista Negra de IP

1) Reglas de Lista Negra

Puede añadir los tipos de las reglas para la Lista Negra de IP como quieres.

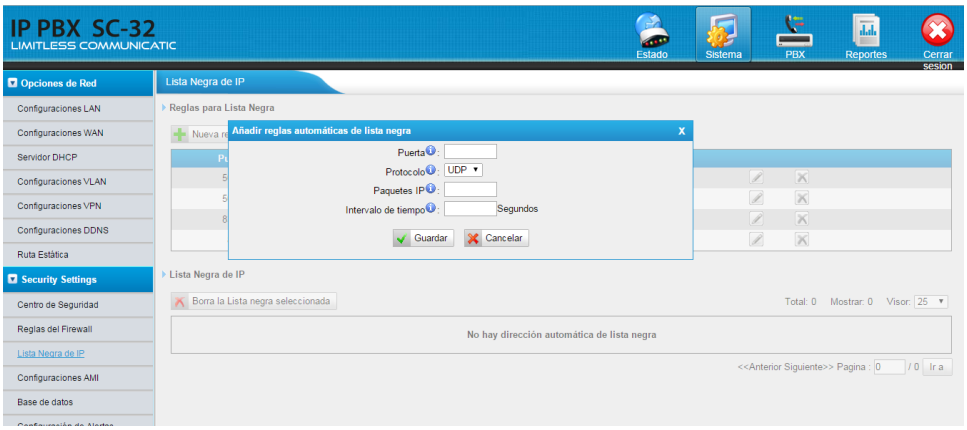


Figura 5-14 Agregan Reglas de Lista Negra

·Puerto
Puerto de defensa automática

·Protocolo
Protocolo de defensa automática TCP o UDP.

·Paquetes IP
Número de paquetes IP permitido en el tiempo intervalo específico.

·Tiempo intervalo
El tiempo intervalo a recibir paquetes IP. Por ejemplo, paquetes IP “90”, tiempo intervalo “60” significan 90 paquetes IP son permitidos en 60 segundos.

2) Lista Negra de IP
La dirección IP bloqueada se aparecerá aquí, puede eliminarla como quiere.

5.2.4 Configuraciones de AMI

The Asterisk Manager Interface (AMI) es un sistema de interface supervisión y gestión proporcionado por Asterisk. Permite el monitoreo en vivo de los eventos que ocurren en el sistema, así que le permite solicitar que Asterisk realizar alguna acción. Las acciones que están disponibles son muy variados e incluyen cosas tales como devolver información de estado y originar llamadas nuevas. Muchas aplicaciones interesantes se han desarrollado basada Asterisk que se aprovechan de la AMI como su interfaz principal hacia Asterisk.
Hay dos tipos principales de mensajes en la interfaz del administrador de Asterisk: Sucesos del administrador y acciones del administrador.
El software de la tercera parte puede funcionar con UNI-K mediante interface AMI. Está desactivado por defecto. Si es necesario, puede habilitarlo.

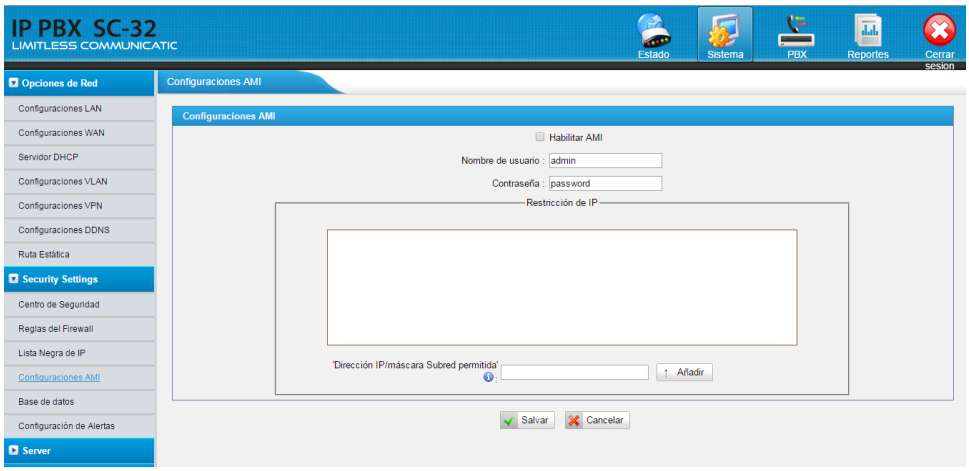


Figura 5-15 Configuraciones de AMI

Nombre de usuario & contraseña: después de habilitar AMI, puede entrar en AMI de UNI-K con este nombre de usuario y contraseña.

Restricción de IP: puede establecer las IP con qué puede iniciar sesión en la interface de IAM de UNI-K.

5.2.5 Donación de Database

IP PBX SC-32 están utilizando database MySQL desde 14.18.0.22. El software de la tercera parte puede acceder a MySQL por vía internet. Antes de eso, es necesario conceder a la autoridad para el usuario de database.

Después de ingresar la página "Donación de Database" , haga clic en "Añadir", puede añadir un usuario de database, establece la contraseña del usuario y conceder la autoridad.

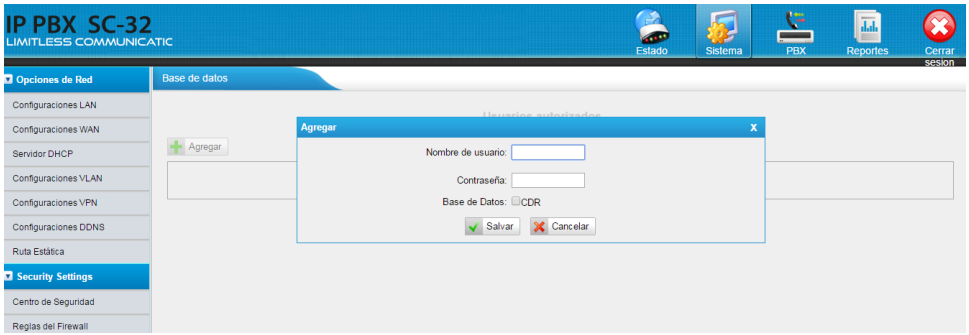


Figura 5.-16 Donación de Database

Nombre del Usuario/contraseñas: La tercera parte puede acceder MySQL utilizando este nombre del usuario y contraseña.

Database: Hay dos opciones, CDR y Record. Si seleccione CDR, entonces este usuario tiene la autoridad a chequear database de CDR; Si seleccione Record, entonces el usuario tiene la autoridad a chequear cuál llamada había grabada automáticamente.

5.2.6 Configuraciones de Alerta

Si el dispositivo sea atacado, el sistema notificará a los usuarios la alerta por vía llamada o E-mail.
Los modos de ataque incluyen ataque de IP y web Login.
Para más detalles sobre la seguridad del sistema y configuración por favor consulta **ANEXO H Guía de Configuración de Seguridad de UNI-K**

Figura 5-17 Configuraciones de Alerta

1. Ataque de IP
Cuando el sistema fue atacado por la dirección IP, el firewall añadirá la IP automáticamente la Lista Negra de IP y notificará al usuario si corresponda a la regla de protección.

1) Configuraciones de Notificación Telefónica

·Notificación Telefónica
Si habilita la notificación telefónica o no.

·Número
El número pueda ser establecido para la notificación alerta; los usuarios puede establecer extensión múltiple y números de teléfono saliente. Por favor separarlos con ";".
Ejemplo: "500;9911", si la extensión ha establecida las configuraciones de Follow Me, la llamada pasará directamente al número transmitido.

·Intentos
Los intentos para marcar un número telefónico cuando no haya respuesta.

·Intervalo
El intervalo entre cada intento para marcar el número telefónico. Debe ser mayor que 3 segundos, el valor predeterminado es 10 segundos.

·Aviso
Los usuarios escucharán el aviso en cuando reciba la notificación telefónica.

2) Configuraciones de Notificación E-mail.

Nota: Por favor asegura que todas las configuraciones de voicemail fueron configuradas correctamente en la página Configuraciones del Sistema -> Configuraciones de Voicemail antes del uso de esta función.

·Notificación E-mail
Si habilita la Notificación E-mail o no.

·Nombre del Receptor
El receptor para la notificación alerta, y las direcciones de email múltiples son permitidos, por favor separarlas con ";".
Ejemplo: jerry@SISTEK.com; jason@SISTEK.com, 456@sina.com .

·Asunto
El asunto del email alerta.

·Contenido del Email
El contenido del texto apoya predefinidas variables. Nombres variables y las instrucciones correspondientes son como las siguientes:

$(HOSTNAME) Host name
$(LOCALIP) Dirección IP Local
$(SOURCEIP) Origen de la dirección IP Ataque
$(DATETIME) Ocurrido
$(USERNAME) Nombre del Usuario (WEBLOGIN efectiva)
$(DESTMAC) Destino MAC de ataques (IPATTACK efectiva)
$(DESTMAC) Destino del número del Puerto de ataques (IPATTACK efectiva)
$(PROTOCOL) Tipo de Protocolo (IPATTACK efectiva)
$(INTERFACE) Nombre de interface de red (IPATTACK efectiva)

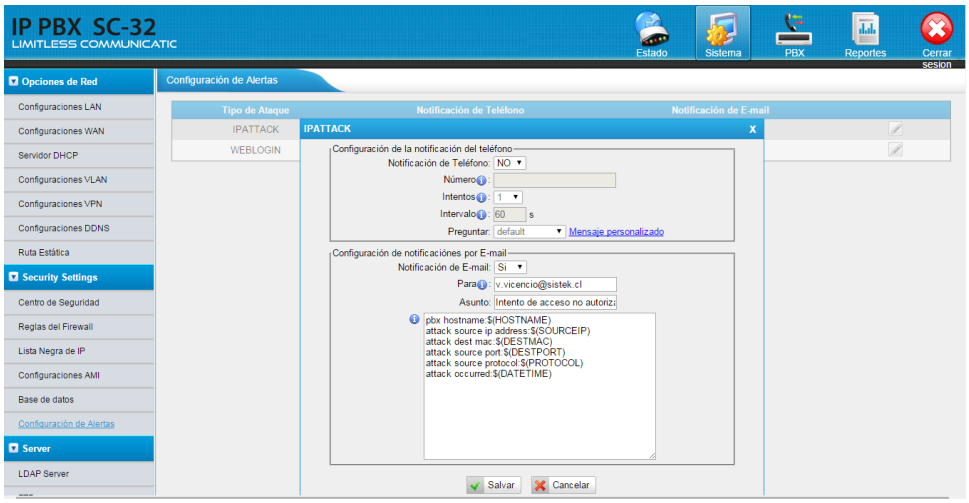


Figura 5-18 Configuración de IP Ataque

2. WEBLOGIN

Notificación de Alerta de Web Login Introduzca la contraseña incorrecta cinco veces a iniciar sesión Web interfaz de UNI-K será considerando como un ataque, el sistema limitará el inicio de sesión IP en 10 minutos y notificará al usuario.

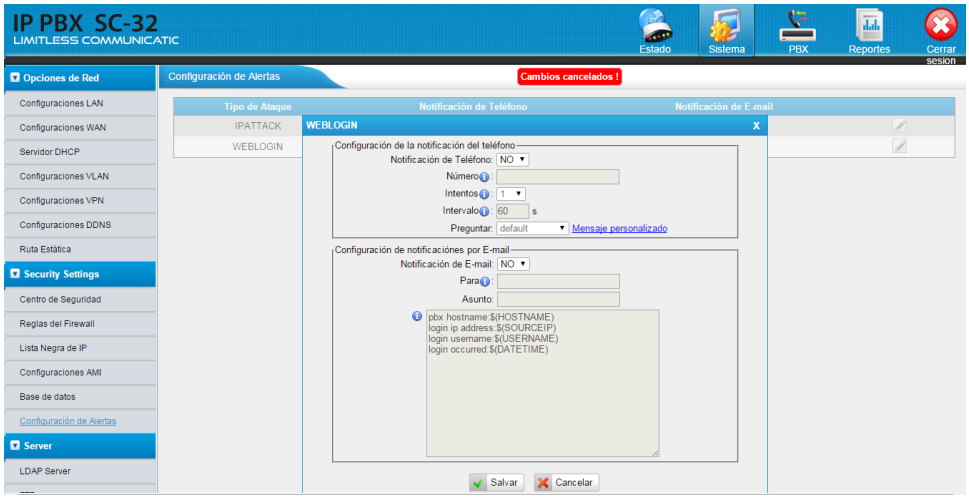


Figura 5-19 Configuración de Alerta de Web Login

5.3 Servidor LDAP

5.3.1 Servidor LDAP

LDAP se utiliza como guía telefónica en UNI-K para que pueda buscar una palabra clave desde su teléfono IP. La palabra clave puede ser un nombre, un número móvil, un email u otra palabra clave en la guía telefónica.

Nota:

Requieren que el teléfono IP debe soportar la función LDAP.

1 Configuraciones de LDAP

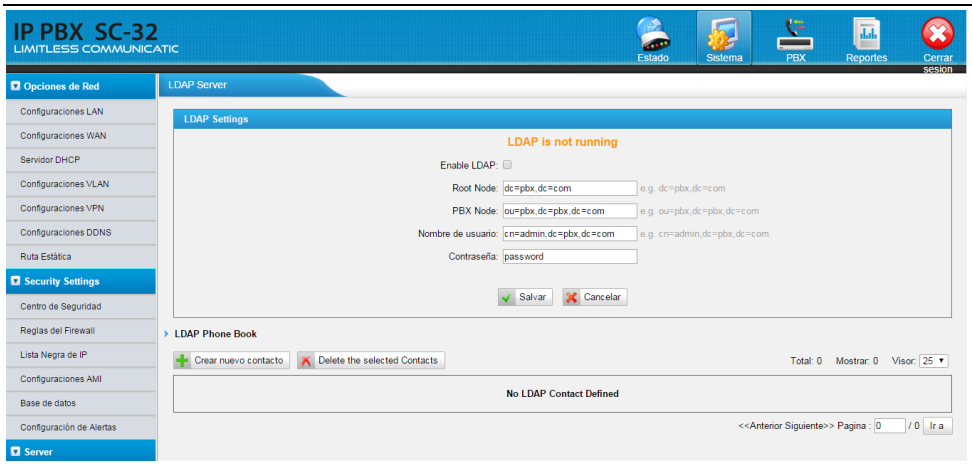


Figura 5-20 Página de Servidor LDAP

·Habilita LDAP

Habilita LADP para usar LDAP en su teléfono IP.

·Nodo Raíz

Un nodo raíz para este LDAP, por ejemplo dc=pbx, dc=com.

·Nodo PBX

Un nodo pbx para este LDAP, por ejemplo ou=pbx, dc=pbx, dc=com.

·Nombre del Usuario

Un usuario para este LDAP, por ejemplo cn=admin, dc=pbx, dc=com.

·Contraseña

Una contraseña utilizando para acceder LDAP.

2) Añadir Contacto

En Añadir Contacto puede crearlos según sea requerido.

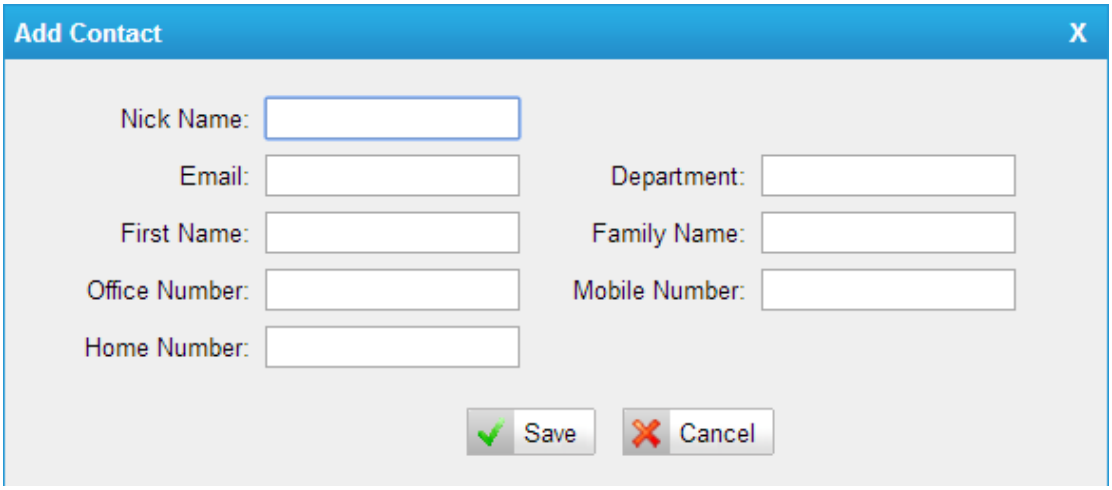


Figura 5-21 Añadir Contacto

Si quiere conocer cómo se usa LDAP, Por favor consulta a ***Appendix J***

5.4 Administración de Almacenamiento

5.4.1 Almacenamiento Externo

La función del Almacenamiento Externo es utilizada para extender el espacio del almacenamiento. Una vez configurado, los archivos (voicemail, archivos de grabación de llamadas) creados antes de la fecha configurada se moverán al Net-Disco.

Nota: La carpeta compartida debe ser basada en el Sistema de Operación Windows. Y si es Windows Vista/2008/7, por favor agrega "Everyone" en la lista de cuenta compartida.

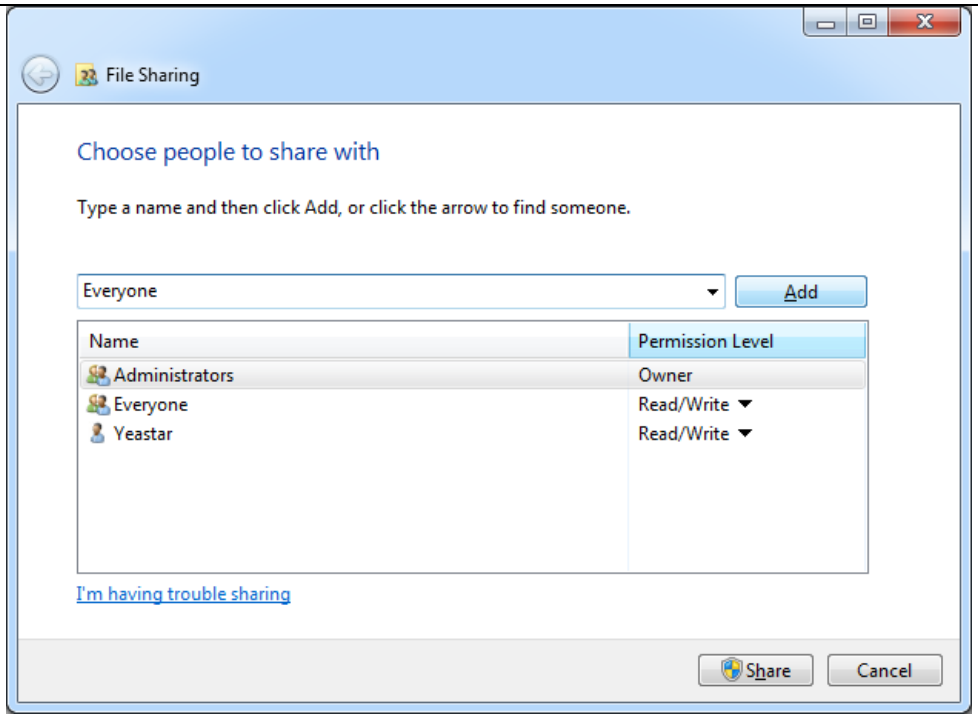


Figura 5-22

Antes del almacenamiento externo puede ser configurado correctamente, una carpeta compartida accesible de SMB desde UNI-K debe configurarse en un equipo basado en Windows. Una vez que han sido configurados, por favor sigue los pasos siguientes.

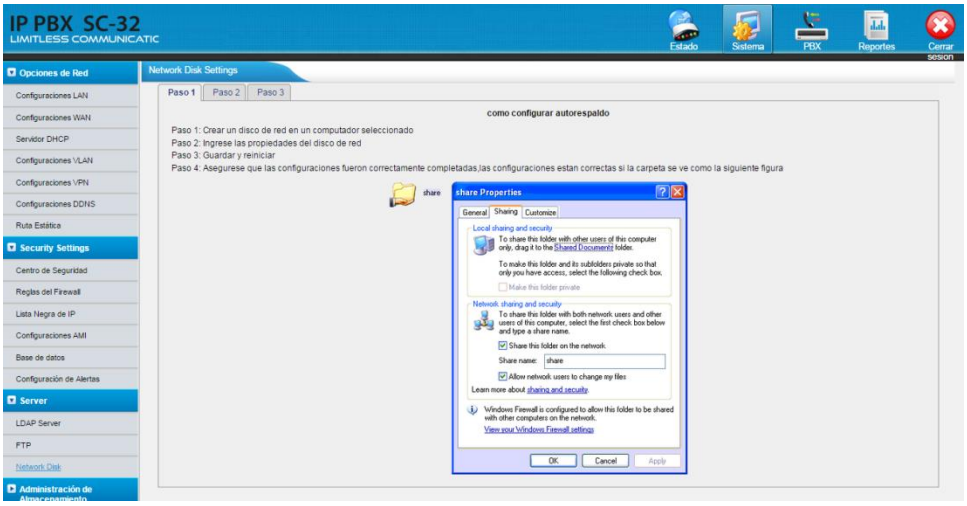


Figura 5-23

Paso 1: Seleccione una computadora basada Windows que está siempre en servicio.
Paso 2: Crear una carpeta
Paso 3: Crear un archivo de texto nombrado "status.txt" en la carpeta
Paso 4: Compartir esta carpeta

Luego debemos introducir la información del Net-Disco en la página de Paso2.

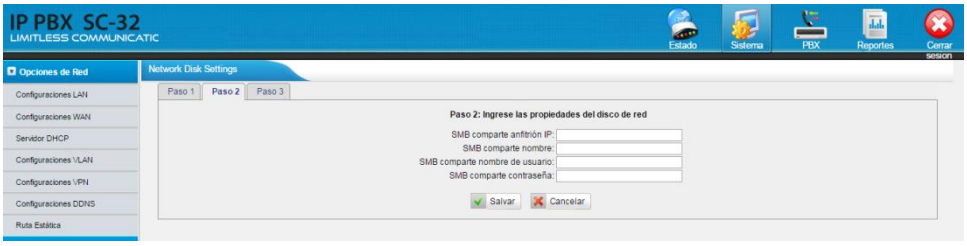


Figura 5-24

Host/IP del Net-Disco: Cambie esto a la dirección IP de la computadora en dónde se almacenarán los archivos de copia de seguridad.

Nombre del Net-Disco Compartido: Cambie esto al nombre de la carpeta compartida en dónde se almacenarán las copias de seguridad.

Nombre del Usuario del Net-Disco Compartido: El nombre del usuario se utiliza para registrarse en la red compartida. Dejase en blanco si no lo requiere.

Contraseña del Net-Disco Compartido: La contraseña se utiliza para registrarse en la red compartida. Dejase en blanco si no lo requiere.

Si la configuración es correcta, abre la carpeta de Windows compartida usted verá las carpetas y archivos de respaldos de UNI-K han sido creados. Si el contenido de la carpeta de copia de seguridad tiene un aspecto similar a la página de Paso3, entonces ha configurado correctamente el almacenamiento externo de la unidad UNI-K.

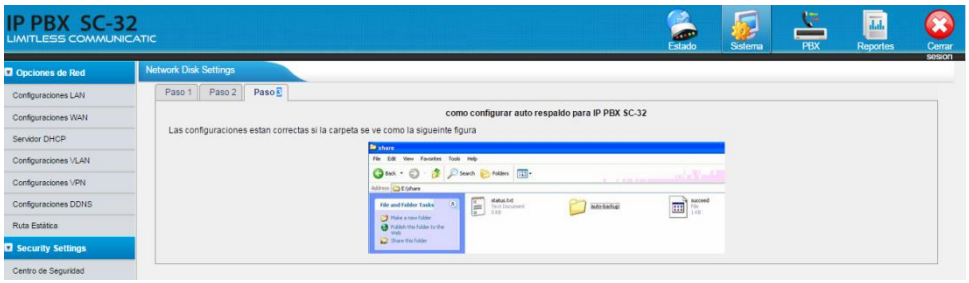


Figura 5-25

5.5 Preferencias del Sistema

En esta página, podemos establecer otras preferencias del sistema, tal como contraseña para la cuenta del admin, fecha y tiempo del sistema, actualización del firmware, reserva en caliente, copia de seguridad y restaurar, restablecer y

reiniciar.

5.5.1 Configuraciones de Contraseña

UNI-K tiene 3 cuentas: Admin, usuario, y cdr. La cuenta de usuario y cdr esta desactivada por defecto.

Cuenta Admin:

La contraseña predeterminada de la cuenta "admin" es "**password**". Para cambiar la contraseña, seleccione "admin" en "Usuario", ingresa la contraseña anterior y la nueva, y haga clic en "guardar". El sistema avisará luego a usted para reiniciarse la sección con su contraseña nueva.

Después de ingresar la contraseña nueva, UNI-K le avisará la fortaleza de la contraseña. Se recomienda el uso de números, letras mayúsculas y minúsculas para aumentar la seguridad.

Al iniciar sesión en UNI-K con la cuenta "admin", puede activar la cuenta de "usuario" y "cdr"; También, puede cambiar sus contraseñas.

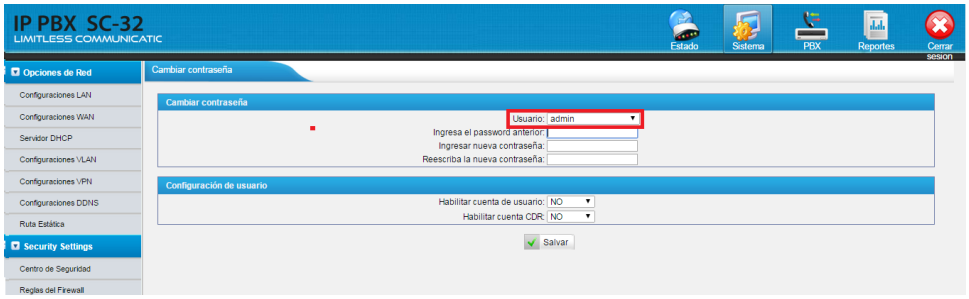


Figura 5-26

Cuenta del Usuario:

La cuenta del usuario está desactivada por defecto y su contraseña predeterminada es "password". Al habilitar la cuenta de "usuario" por primera vez, UNI-K le pedirá que cambie la contraseña de "usuario". Si no la cambie, no se puede habilitar la cuenta de "usuario".

Para cambiar la contraseña, seleccione "usuario" en "usuario", ingresa la contraseña anterior y la nueva, y haga clic en "guardar". El sistema avisará luego a usted para reiniciarse la sección con su contraseña nueva.

Después de ingresar la contraseña nueva, UNI-K le avisará la fortaleza de la contraseña. Se recomienda el uso de números, letras mayúsculas y minúsculas para aumentar la seguridad.

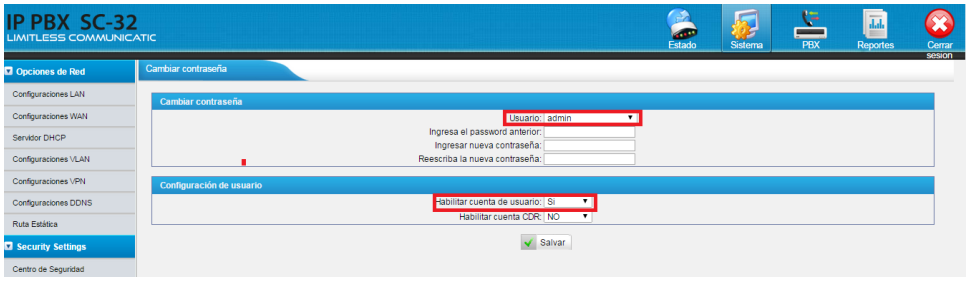


Figura 5-27

Después de habilitar la cuenta de "usuario", puede registrarse en UNI-K con "usuario". La cuenta de "usuario" puede cambiar su contraseña propia.

Cuenta CDR:

La cuenta del "cdr" está desactivada por defecto y su contraseña predeterminada es "password". Puede habilitarla después de registrarse en UNI-K con la cuenta "admin".

Para cambiar la contraseña, seleccione "cdr" en "usuario", ingresa la contraseña anterior y la nueva, y haga clic en "guardar". El sistema avisará luego a usted para reiniciarse la sección con su contraseña nueva.

Después de ingresar la contraseña nueva, UNI-K le avisará la fortaleza de la contraseña. Se recomienda el uso de números, letras mayúsculas y minúsculas para aumentar la seguridad.

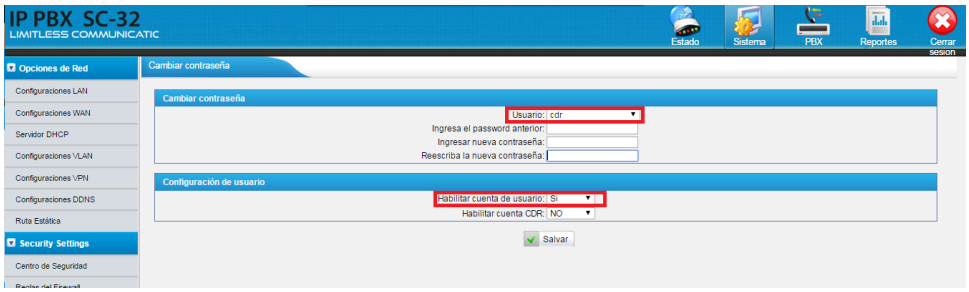


Figura 5-28

Después de habilitar la cuenta de "cdr", puede registrarse en UNI-K con "cdr". La cuenta de "cdr" puede cambiar su contraseña propia.

5.5.2 Fecha y Tiempo

Establece la fecha y tiempo para UNI-K.

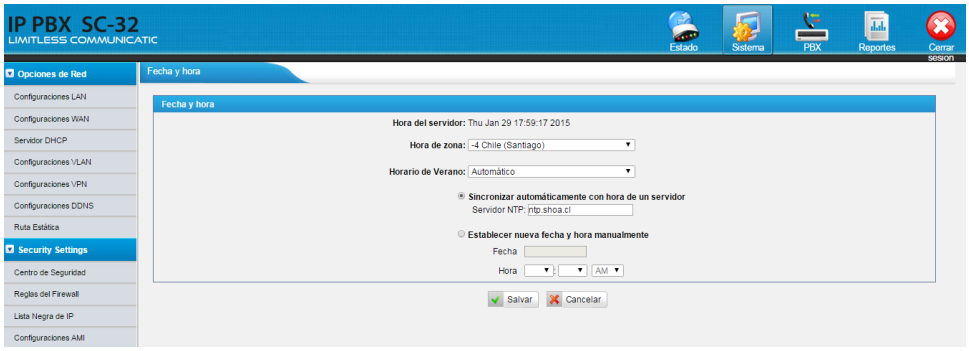


Figura 5-29

·Huso Horario
Puede seleccionar su huso horario aquí.

·Horario de Verano
Establece el modo a automático o desactivado

·Sincronizar automáticamente con un servidor horario de Internet
Introduzca el servidor NTP para que UNI-K actualice la hora automáticamente.

·Establece Fecha & Tiempo Manualmente
Puede establecer el tiempo para su tiempo local correcto manualmente aquí.

5.5.3 Actualización de Firmware

La actualización del firmware es posible a través de la web interfaz de administrador Web usando un servidor TFTP o una URL HTTP.
Ingrese su dirección de IP del servidor TFTP y el nombre del archivo de firmware, haga clic en Iniciar para actualizar el firmware.

Notas:
1. Si "Restablecer configuración a valores predeterminados de fábrica" está habilitado, el sistema restaurará la configuración predeterminada de fábrica.
2. Cuando está actualizando el firmware, por favor no apague la energía. Si no el sistema se dañará.
3. Para más información sobre los pasos de la actualización del firmware, por favor consulte este link:
http://www.unik-latam.com/download/UNI-K-IP PBX SC-32/UNI-K_IP PBX SC-32_FirmwareUpgrade_en.pdf

Figura 5-30

5.5.4 Copia de Seguridad y Restaurar

Podemos copiar de seguridad de las configuraciones antes de restablecer UNI-K IP PBX SC-32 a los valores de fábrica, y luego restaurarlo usando este paquete. La copia de seguridad creada en UNI-K se cifra con formato de archivo ".bak".

Notas:

1. Solamente configuraciones, mensajes personalizados serán respaldados, los archivos de correo de voz y grabación no están incluidos.
2. Cuando ha actualizado la versión del firmware, no se recomienda a restaurar utilizando el paquete viejo.

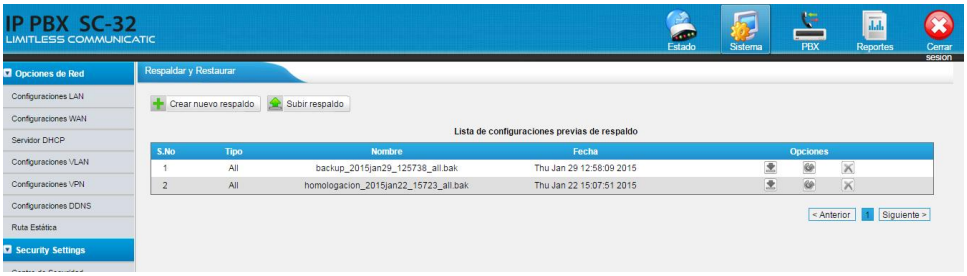


Figura 5-31

·Crear una Copia de Seguridad Nueva

Los usuarios pueden crear una copia de seguridad nueva para "Todos" o extensiones separadas.

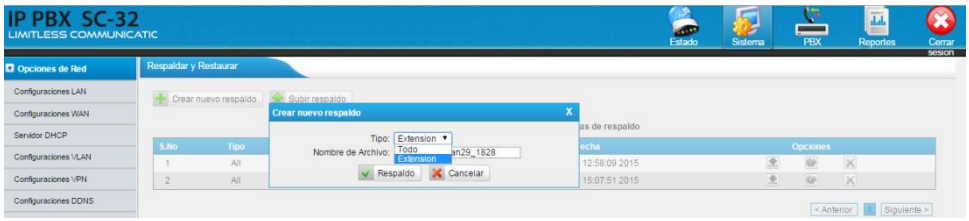


Figura 5-32

·Cargar una Copia de Seguridad

Los usuarios pueden cargar una copia de seguridad para "Todos" o extensiones separadas.

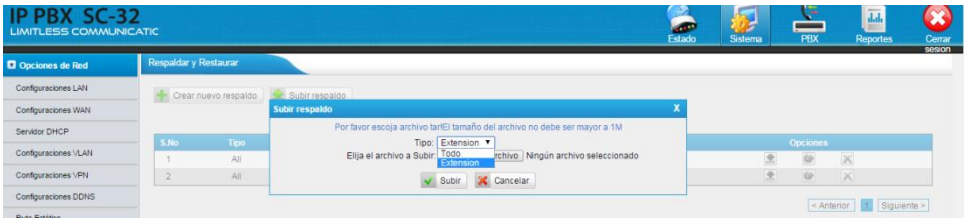


Figura 5-33

5.5.5 Restablecer y Reiniciar

Podemos restablecer o reiniciar UNI-K IP PBX SC-32 por vía web directamente en esta página.

IP PBX SC-32
Estado
Sistema
PBX
Reportes
Cerrar sesion
Opciones de Red
Reiniciar el dispositivo y Restablecer a los valores
Reiniciar el dispositivo
Reiniciar el dispositivo
Advertencia: reiniciar el dispositivo cancelara todas las llamadas activas.
Reiniciar
Restablecer a predeterminado de fabrica
Restablecer a predeterminado de fabrica
Advertencia: Por restaurar su sistema a los valores predeterminados de fábrica, se perderán todas las configuraciones!
No se puede cortar la electricidad durante el reinicio hasta que el estado RUN parpadee la luz, de lo contrario hará que falle el procedimiento.
Restablecer valores predeterminados

Figura 5-34

·Reiniciar el Sistema

Advertencia: El reinicio del sistema terminará todas las llamadas activadas.

·Restablecer a los Valores Predeterminados de Fábrica

Advertencia: Un restablecimiento a fábrica borrará todos los datos de configuración del sistema.

Por favor, no apague el sistema hasta que la luz RUN comienza a parpadear. Cualquier interrupción de la energía durante este tiempo podría causar daños al sistema.

6. PBX

Haga clic

a acceder ficha de “PBX”.

En esta página, se puede configurar las configuraciones de extensión, tronco, control de llamadas entrantes, control de llamadas salientes, la configuración de audio y los demás. Después de la configuración, podemos hacer o recibir llamadas como programado.

6.1 Extensiones

En esta página, podemos configurar los detalles de las extensiones y provisión de los modelos soportados automáticamente.

6.1.1 Extensiones FXS/VoIP

Hay tres tipos de extensiones soportadas en UNI-K IP PBX SC-32 V5: SIP, IAX y análogo extensión.

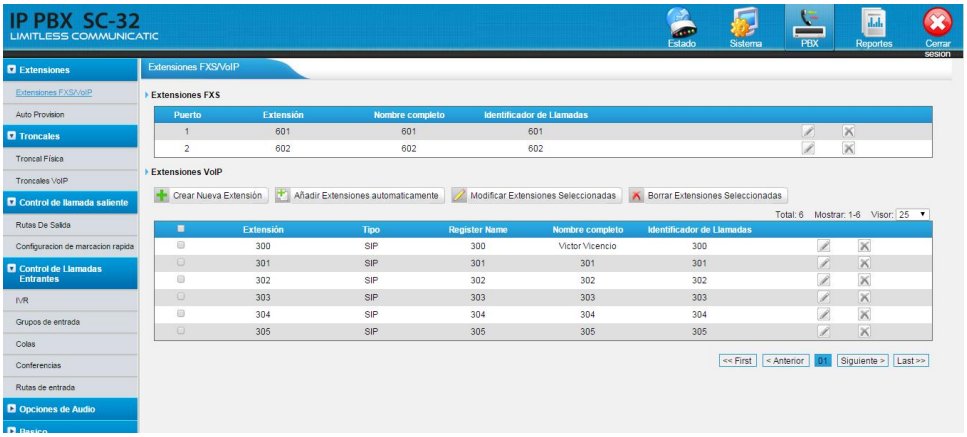


Figura 6-1

FXS Extensiones

Figura 6-2 FXS

Hay dos extensiones analógicas en UNI-K IP PBX SC-32 V5 si está instalado el módulo S2, para modificar el número de extensión, elimínelo primero y volver a crearlo.

1) General

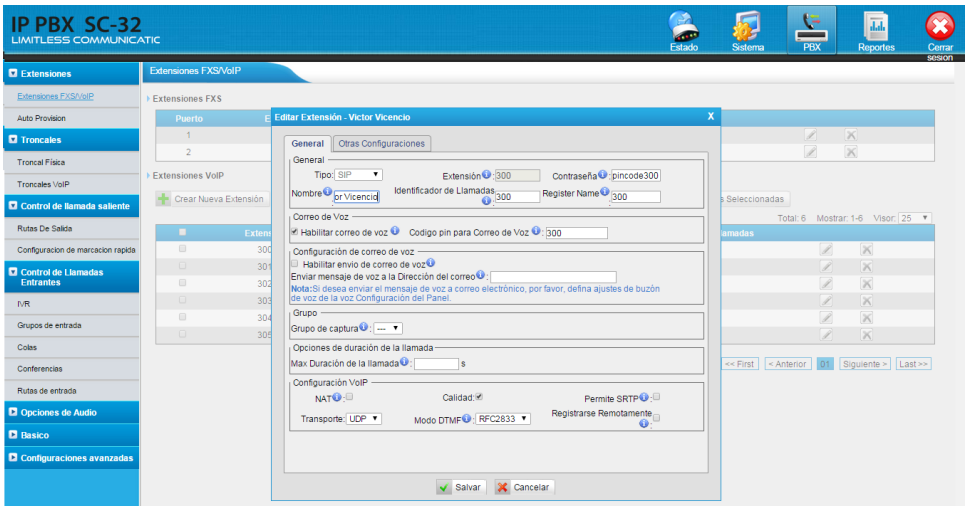


Figura 6-3

·Extensión
La extensión numerada, por ejemplo, 1234, que se asociará con este usuario / teléfono particular. The numbered extension,

·Puerto
El puerto correspondiente de la extensión.

·Nombre
Un nombre basado en caracteres para este usuario, por ejemplo, "Bob Jones".

·Identificador de Llamada
La cadena del Identificador de Llamada (CID) se utilizará cuando el usuario llama a otro usuario interno.

2) Voicemail

·Habilita Voicemail

Revisa esta casilla si el usuario debe tener una cuenta de voicemail.

·Acceso PIN # de Voicemail

La contraseña de voicemail para esta extensión, por ejemplo, "1234".

3) Configuración de Mail

·Habilita Enviar Voicemail

Una vez activado, el voicemail será enviado a la dirección de email a continuación como un archivo adjunto.

·Enviar Voicemail a la Dirección de Email

Esta opción define si los voicemails/fax se envían a la dirección de Email como archivo adjunto.

Nota: Por favor asegura que todas las configuraciones de voicemail fueron configuradas correctamente en la página Configuraciones del Sistema -> Configuraciones de Voicemail antes del uso de esta función.

4) Flash

·Detección de Hook Flash

Establece la cantidad de tiempo, en milisegundos, que debe transcurrir desde el último evento de gancho-flash recibida por UNI-K antes de que reconozca un segundo evento. Si un segundo evento se produce en menos tiempo que se define por detección de Hook Flash, entonces UNI-K ignorará el evento. El valor predeterminado de Flash es 1000ms, y se puede ser configurado en 1ms incrementos.

5) Grupo

·Grupo Pickup

Si esta extensión pertenece a un grupo de pickup, a las llamadas que suenan esta extensión pueden ser recogidos por otras extensiones que están en el mismo grupo de pickup marcando el código de función de Pickup (el valor predeterminado es *4).

Nota: *4 es la configuración predeterminada, puede cambiarlo abajo de Código de Función -> General -> Llamada Pickup.

6) Configuración de la Duración de Llamada

Configura la duración sacrificio máximo para cada llamada de esta extensión, pero es sólo válido para las llamadas salientes. Introduzca "0" o dejarlo en espacio vacío, el valor sería igual a la duración de la llamada Max configurado en la página Configuración de opciones.

Nota: Esta configuración no será válida para las llamadas internas.

Otras Configuraciones

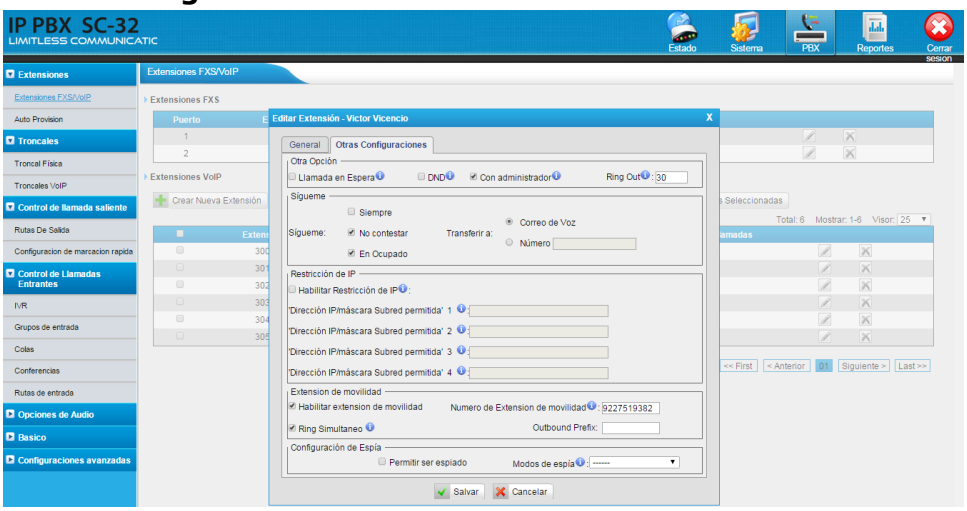


Figura 6-4

7) Otras opciones

·Llamada en Espera

Marque esta opción si la extensión debe tener la capacidad de llamada en espera. Si esta opción está marcada, "cuando está ocupada" de la opción de Follow me será inválida.

·DND

No Molesta.

·Web Interfaz del Usuario

Marque esta opción para permitir al usuario a iniciar sesión en la web interfaz de usuario UNI-K, que puede ser utilizado para revisar correo de voz y grabaciones de extensión. Los usuarios pueden iniciar sesión de la interfaz web de usuario UNI-K utilizando su número de extensión y PIN de correo de voz como el nombre de usuario y contraseña, respectivamente.

·Resuenan

Marque esta opción si quiere personalizar el tiempo del timbre. El tono se parará hasta el tiempo definido.

8) Sígueme (Desvío de llamadas)

Esta función se establece el reenvío de llamadas entrantes en una extensión. Un administrador puede configurar sígueme para esta extensión.

9) Configuraciones del Volumen

Rxgain: El volumen enviado a la extensión FXS.

Txgain: El volumen enviado por la extensión FXS.

10) Extensión Móvil
UNI-K le permite a utilizar tu teléfono móvil como una extensión. Si establece su teléfono móvil como una extensión móvil y entonces puede llamar a UNI-K con este teléfono móvil, escuchará un tono de marcación. UNI-K considerará su llamada como una llamada viene de una extensión. Puede marcar el número de otras extensiones (su ID de llamada será el número de su extensión) o marcar por vía ruteo saliente como marcando desde su extensión.

Nota: Si callback está habilitada en la route entrante, la función de extensión móvil de este route entrante se desactivará.

Habilita la Extensión Móvil
Habilita esta función.

·Número de la Extensión Móvil
Cuando usted marca el servidor con este número, el teléfono móvil recibe el permiso de la extensión. Por ejemplo: marcar las otras extensiones, reproduciendo el correo de voz.

·suenan simultáneamente
Cuando la extensión tiene una llamada entrante, suena su extensión móvil simultáneamente.

·Prefijo Saliente
Rellena un prefijo apropiado del número de teléfono móvil para que pueda coincidir con un route saliente para marcar la extensión de la móvil. Por ejemplo, si establece el prefijo a "9", enviará "9 + el número de extensión móvil" al route saliente.

11) Tipo de ID de Llamada
Configuración de ID de Llamada
Normalmente, se elige la opción "por defecto" excepto por el uso UNI-K en Japón, en cuyo caso usted debe elegir "Japón".

12) Configuraciones Monitoreo
UNI-K permite la extensión a monitorear / barcaza en otra conversación. Una vez que esta función está activada, la extensión tiene la capacidad de monitorear / barcaza en otras llamadas utilizando los códigos de funciones para cada modo de monitoreo. Consulta a la sección de “Códigos de Función” para más información.

·Modos de Monitoreo

Hay 4 modos disponibles de monitoreo:
Monitoreo general: puede tener el permiso a utilizar los siguientes 3 modos.
Monitoreo normal: solamente puede escuchar la llamada, pero no puede hablar.
Monitoreo susurro: puede escuchar la llamada, y puede hablar con la extensión monitoreada.
Monitoreo barcaza: puede escuchar la llamada y hablar con las ambas partes.

Nota: por ejemplo, si 500 quieren monitorear la extensión 501, tenemos que activar la opción "permitir ser monitoreado" por 501, y elija el modo de monitoreo para la extensión 500.
Luego recoger 500 y marque "códigos de función + 501" para iniciar el monitoreo cuando 501 está en una llamada.
Si 500 elige "monitoreo normal", debe marcar "* 90501" para iniciar el monitoreo.
Si 500 elige "monitoreo susurro", debe marcar "* 91501" para iniciar el monitoreo.
Si 500 elige "monitoreo barcaza", debe marcar "* 92501" para iniciar el monitoreo.
Si 500 elige "monitoreo general", puede marcar "*90501", "*91501" o "*92501" para iniciar el monitoreo.

Extensiones VoIP

Una Extensión VoIP es una cuenta SIP/IAX que permita un teléfono IP o cliente de un Soft-teléfono registrase en UNI-K.

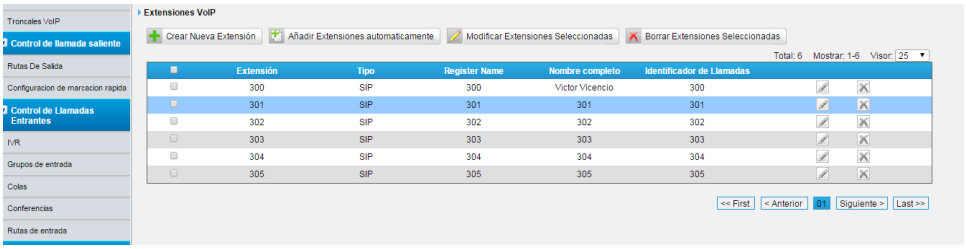


Figura 6-5

Podemos hacer clic en "Añadir extensión" para empezarnos.

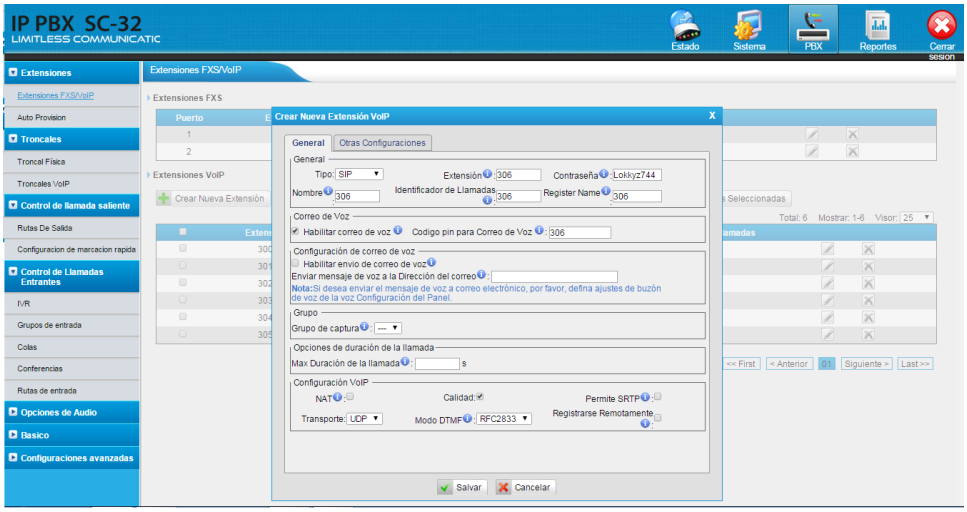


Figura 6-6

1) General

·Tipo

Tipo de Extensión: SIP, IAX o SIP/IAX.

SIP – La extensión envía y recibe llamadas utilizando el protocolo SIP de VoIP.

IAX – La extensión envía y recibe llamadas utilizando el protocolo IAX de VoIP.

·Extensión

La extensión numerada, por ejemplo, 1234, que se asociará con este usuario / teléfono particular.

·Contraseña

La contraseña para esta extensión, pero no es una fija. Cuando agrega una extensión nueva, una contraseña aleatoria y robusta se generará como "Gtwfup642".

·Nombre

Un nombre basado en caracteres para este usuario, por ejemplo, "Bob Jones".

·Identificador de Llamada

El Identificador de Llamada se utilizará cuando el usuario llama a otra extensión interna.

·Nombre Registro

Es para la validación de registro de extensión. Los usuarios no podrán registrar la extensión si el nombre de autorización es incorrecto incluso cuando el nombre de usuario y la contraseña son correctos.

2) Voicemail

·Habilita Voicemail

Revisa esta casilla si el usuario debe tener una cuenta de voicemail.

·Acceso PIN de Voicemail

La contraseña de voicemail para esta extensión, por ejemplo, "1234".

3) Configuración de Mail

Esta opción define si los voicemails/fax se envían a la dirección de Email como archivo adjunto.

·Habilita Enviar Voicemail

Una vez activado, el voicemail será enviado a la dirección de email como un archivo adjunto.

·Dirección de Email

La dirección de Email está utilizando para recibir el voicemail o Fax.

Nota: Por favor, asegúrese de que la sección "Configuración de SMTP para el Voicemail" (en "Configuración del Voicemail") se han configuradas correctamente antes de utilizar esta característica.

4) Grupo

·Grupo Pickup

Si esta extensión pertenece a un grupo de pickup, a las llamadas que suenan esta extensión pueden ser recogidos por otras extensiones que están en el mismo grupo de pickup marcando el código de función de Pickup (el valor predeterminado es *4).

Nota: *4 es la configuración predeterminada, puede cambiarlo abajo de Código de Función -> General -> Llamada Pickup.

5) Configuraciones de la Duración de Llamada

Configura la duración sacrificio máximo para cada llamada de esta extensión, pero es sólo válido para las llamadas salientes. Introduzca "0" o dejarlo en espacio vacío, el valor sería igual a la duración de la llamada Max configurado en la página Configuración de opciones.

Nota: Esta configuración no será válida para las llamadas internas.

6) Configuraciones VoIP

·NAT

Esta configuración debe utilizarse cuando el sistema está usando una dirección IP pública para comunicarse con dispositivos ocultos detrás de un dispositivo NAT (como un router de banda ancha). Si tiene problemas de un solo sentido de

audio, que por lo general tienen problemas con su configuración NAT o el soporte de su firewall de SIP y/o puertos RTP.

·Calificar
Enviar los paquetes de comprueba vivas a teléfonos IP

·Habilita SRTP
Habilita Extensión para for SRTP (RTP Encryption).

·Transporte
Este será el método de transporte utilizado por la extensión. Estas opciones son UDP (Por defecto) o TCP o TLS.

·DTMF Modo – RFC2833, Info, Inband, Auto.

·Registro Remoto
Permite el registro remoto de las extensiones.
Si habilita "Registro Remoto", la contraseña de la extensión debe incluir letras mayúsculas, minúsculas y números.
Esta opción se utiliza para mejorar la seguridad del sistema, que está desactivado por defecto.
Para más detalles sobre la configuración de la seguridad del sistema, por favor consulta **APPENDIX H UNI-K Security Configuration Guide**

Otras opciones

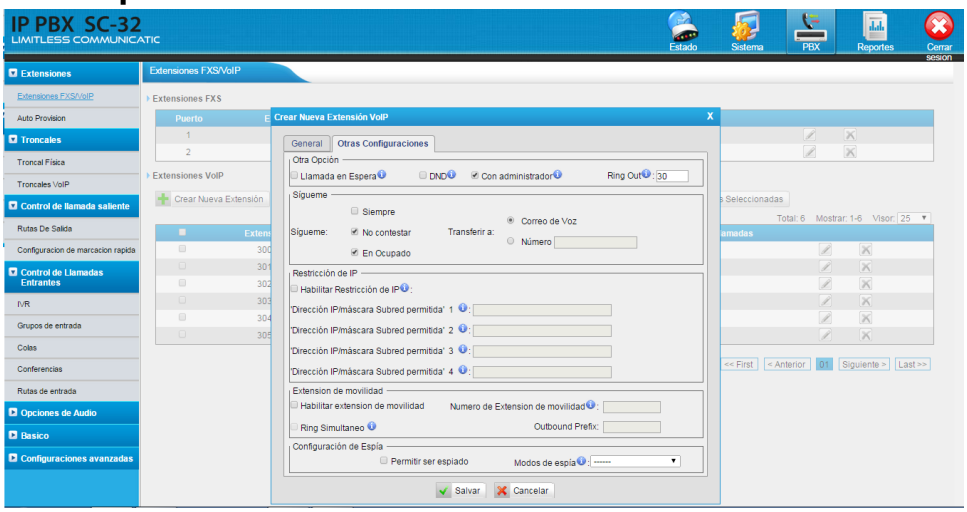


Figura 6-7

7) Otras opciones

·Llamada en Espera
Marque esta opción si la extensión debe tener la capacidad de llamada en espera. Si esta opción está marcada, "cuando está ocupada" de la opción de follow me

será inválida. La función de llamada en espera del teléfono IP tiene mayor prioridad que la función de llamada en espera de UNI-K.

·DND
No Molesta. Cuando DND está habilitado en una extensión, la extensión será indisponible.

·Web Interfaz del Usuario
Marque esta opción para permitir al usuario a iniciar sesión en la web interfaz de usuario UNI-K, que puede ser utilizado para revisar correo de voz y grabaciones de extensión. Los usuarios pueden iniciar sesión de la interfaz web de usuario UNI-K utilizando su número de extensión y PIN de correo de voz como el nombre de usuario y contraseña, respectivamente.

·Resuenan
Marque esta opción si quiere personalizar el tiempo del timbre. El tono se parará hasta el tiempo definido.

8) Sígueme (Desvío de llamadas)
El desvío de llamadas para una extensión se puede configurarse aquí. Un administrador puede configurar sígueme para esta extensión. Si desea transferir la llamada a un número saliente, por favor siga el patrón de marcación de route saliente llena en el número saliente.
Por ejemplo: la transferencia de una llamada a su número de teléfono móvil 123456789, el patrón de marcación de route saliente es "9"., Hay que rellenar 9123456789 aquí.

9) Restricción IP
·Habilita Restricción IP
Marque esta opción para mejorar la VoIP seguridad para UNI-K. Si esta opción está habilitada, solamente la IP/Subnet mask permitida puede registrarse este número de la extensión. De esta manera, se mejorará la seguridad de VoIP.
Para más detalles sobre la configuración de la seguridad del sistema, por favor consulta **APPENDIX H UNI-K Security Configuration Guide**.

·"Dirección IP/Subnet mask" Permitida
El formato de entrada debe ser "dirección IP" + "/" + "Máscara de subred".
Por ejemplo, "192.168.5.100/255.255.255.255" significa solamente el dispositivo que cuya dirección IP es 192.168.5.100 está permitido registrarse este número de extensión.
Por ejemplo, "192.168.5.0/255.255.255.0" significa solamente el dispositivo que cuya dirección IP es 192.168.5.XXX está permitido registrarse este número de extensión.

10) Extensión Móvil

UNI-K le permite a utilizar tu teléfono móvil como una extensión. Si establece su teléfono móvil como una extensión móvil y entonces puede llamar a UNI-K con este teléfono móvil, escuchará un tono de marcación. UNI-K considerará su llamada como una llamada viene de una extensión. Puede marcar el número de otras extensiones (su ID de llamada será el número de su extensión) o marcar por vía ruteo saliente como marcando desde su extensión.

Nota: Si callback está habilitada en la route entrante, la función de extensión móvil de este route entrante se desactivará.

·Habilita la Extensión Móvil

Habilita esta función.

·Número de la Extensión Móvil

Cuando usted marca el servidor con este número, el teléfono móvil recibe el permiso de la extensión. Por ejemplo: marcar la otra extensión, reproduciendo el correo de voz.

·suenan simultáneamente

Cuando la extensión tiene una llamada entrante, suena su móvil simultáneamente.

·Prefijo Saliente

Rellena un prefijo apropiado del número de teléfono móvil para que pueda coincidir con un route saliente para marcar la extensión de la móvil. Por ejemplo, si establece el prefijo a "9", enviará "9 + el número de extensión móvil" al route saliente.

11) Configuraciones Monitoreo

UNI-K permite la extensión a monitorear / barcaza en otra conversación. Una vez que esta función está activada, la extensión tiene la capacidad de monitorear / barcaza en otras llamadas utilizando los códigos de funciones para cada modo de monitoreo. Consulta a la sección de “Códigos de Función” para más información.

·Modos de Monitoreo

Hay 4 modos disponibles de monitoreo:

Monitoreo general: puede tener el permiso a utilizar los siguientes 3 modos.

Monitoreo normal: solamente puede escuchar la llamada, pero no puede hablar.

Monitoreo susurro: puede escuchar la llamada, y puede hablar con la extensión monitoreada.

Monitoreo barcaza: puede escuchar la llamada y hablar con las ambas partes.

Nota: por ejemplo, si 500 quieren monitorear la extensión 501, tenemos que activar la opción "permitir ser monitoreado" por 501, y elija el modo de monitoreo para la extensión 500.
Luego recoger 500 y marque "códigos de función + 501" para iniciar el monitoreo cuando 501 está en una llamada.
Si 500 elige "monitoreo normal", debe marcar "* 90501" para iniciar el monitoreo.
Si 500 elige "monitoreo susurro", debe marcar "* 91501" para iniciar el monitoreo.
Si 500 elige "monitoreo barcaza", debe marcar "* 92501" para iniciar el monitoreo.
Si 500 elige "monitoreo general", puede marcar "*90501", "*91501" o "*92501" para iniciar el monitoreo.

6.1.2 Aprisionamiento de Teléfono

El submenú de Auto Provisión proporciona a los usuarios un método para Auto Provisión de Teléfono IP después del proceso de Instalación Express.
Nota: La Función de Auto Provisión está homologada completamente con estos modelos:
Yealink (T12, T18, T19, T20, T21, T22, T26, T28, T32, T38, T41, T42, T46, W52P, VP530, VP-2009)
Snow (300, 320, 360, 370)
Polycom (IP 6000, IP 7000, IP 32X, IP33X, IP430, IP450, IP550, IP560, VVX1500)
Cisco (IP7940, IP7960)
Astra (9480i, 9480i-CT, 6730i, 6731i, 6737i, 6753i, 6755i, 6757i, 6757i CT)
Grand Stream (GXP1450, GXP2100, GXP2110, GXP2120)
Escene (ES220, ES320, ES330, ES410, ES620)
Fanvil (C56, C58, C60, C62)
Panasonic (UT113, UT123, UT133, UT136, UT248, UT670, TGP500, TGP550)

Noticias:
Cuando aprovisiona teléfono IP de Yealink, Grandstream, Fanvil, Snom, UNI-K no es necesario a ser establecida como el servidor DHCP ínico más.

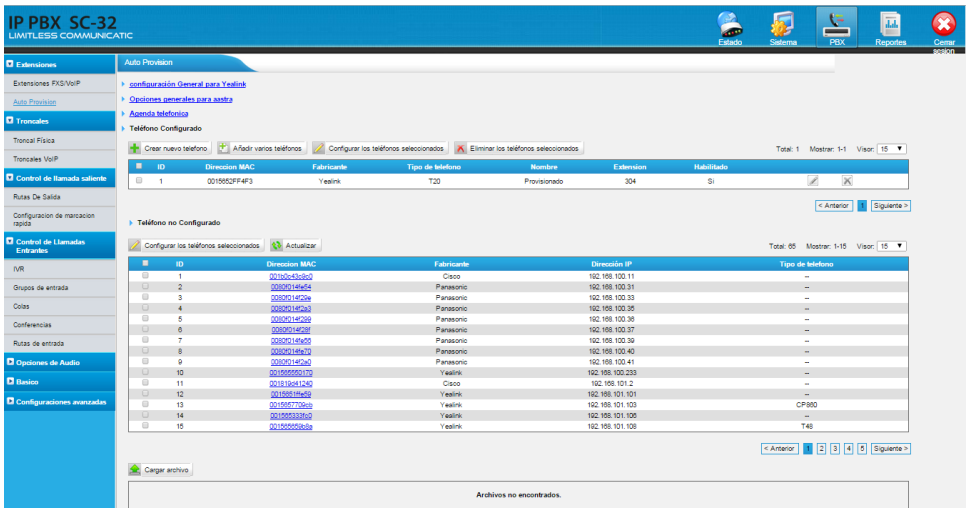


Figura 6-8

6.1.2.1 Configuraciones Generales para Yealink

En esta página, puede ajustar las configuraciones generales antes de aprovisionar los teléfonos IP de Yealink, incluyendo los artículos como preferencias generales, códigos, directorio telefónico remoto y actualiza firmware.

Nota: si el servicio de descarga de firmware está activado, el teléfono IP se actualizará el firmware de forma automática según la versión y el servidor se ha configurado durante el proceso de provisión.

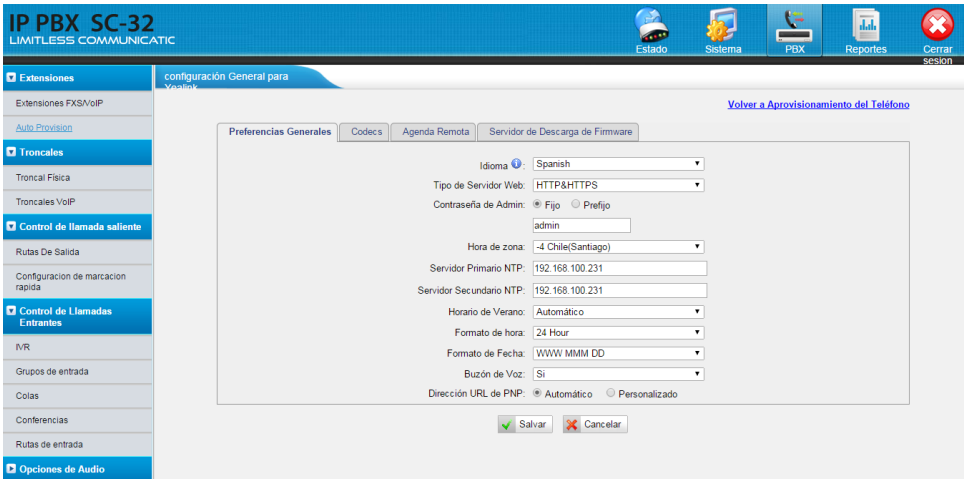


Figura 6-9

6.1.2.2 Configuraciones Generales de Astra

En esta página, puede ajustar las configuraciones generales antes de aprovisionar los teléfonos IP de Astra, incluyendo los artículos como preferencias generales, Configuración del programa claves, configuración de soft claves.

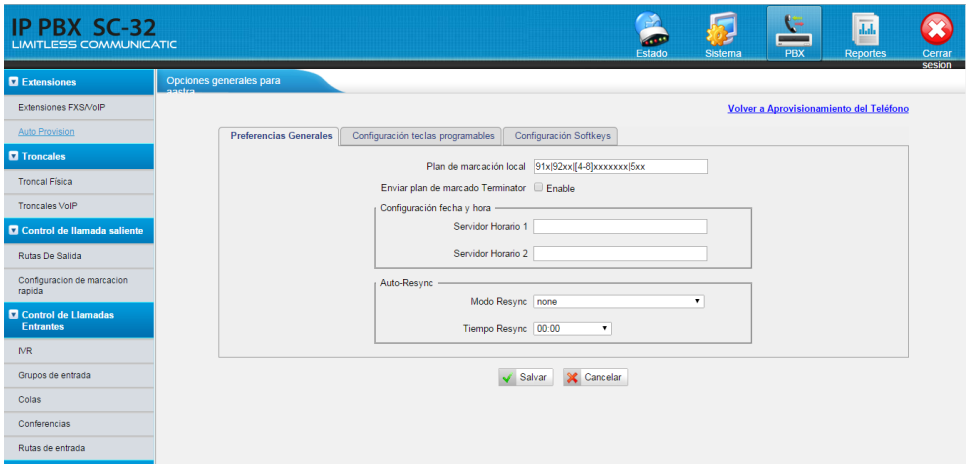


Figura 6-10

6.1.2.3 Directorio Telefónico

Puede añadir sus contactos aquí y cuando utiliza provisión de teléfono; el teléfono IP cargará el directorio telefónico.

Figura 6-11

1) Añadir Contacto

·Tipo

Hay tres tipos: Ninguno, VIP y lista Denegar (lista negra).

·Grupo

Hay 5 grupos: Ninguno, Amigos, Familia, Trabajo, lista Colegas.

·Nombre Nick

Puede establecer un nombre Nick para este número.

·Favorito

Sólo funciona con el teléfono Snom.

·Organización

Introducir la organización de este contacto. Sólo funciona con el teléfono Snom.

·Título

Introducir el título de este contacto. Sólo funciona con el teléfono Snom.

·Email

Introducir el email de este contacto. Sólo funciona con el teléfono Snom.

·Cumpleaños

Introducir el cumpleaños de este contacto. Sólo funciona con el teléfono Snom.

·Primer Nombre

Introducir el primer nombre de este contacto. Sólo funciona con el teléfono Snom.

·Apellido

Introducir el apellido de este contacto. Sólo funciona con el teléfono Snom.

·Número de Oficina

Introducir el número de oficina aquí.

·Número Móvil

Introducir el número móvil aquí.

·Número de Casa

Introducir el número de casa aquí.

·Sub Número

Añadir sub número de este contacto. Sólo funciona con el teléfono Snom.

·Nota

Lleva unas notas de este contacto. Sólo funciona con el teléfono Snom.

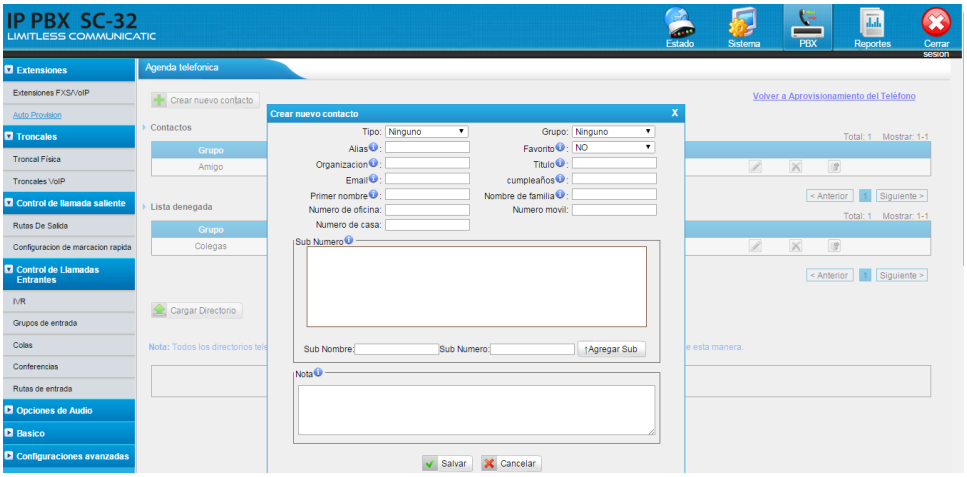


Figura 6-12

2) Cargar Directorio Telefónico

Puede cargar un directorio telefónico antes de la provisión automática, que será aprovisionado para el teléfono IP al utilizar la función provisión automática para configurar sus teléfonos IP. El formato del directorio telefónico debe ser *.xml.

Nota: Todos los directorios telefónicos existentes del teléfono IP, serán reemplazado automáticamente si los directorios telefónicos están configurados en esta manera.

6.1.2.4 Configura Teléfono

Tomemos aprovisionamiento de teléfono Yealink como un ejemplo.
Hay dos modos de crear teléfonos nuevos: crear teléfonos nuevos en la página web y cargar el archivo de configuración del teléfono IP.

Añadir teléfonos nuevos vía página web

Haga clic en "Añadir Teléfono" y complete la información correspondiente en la ventana emergente.

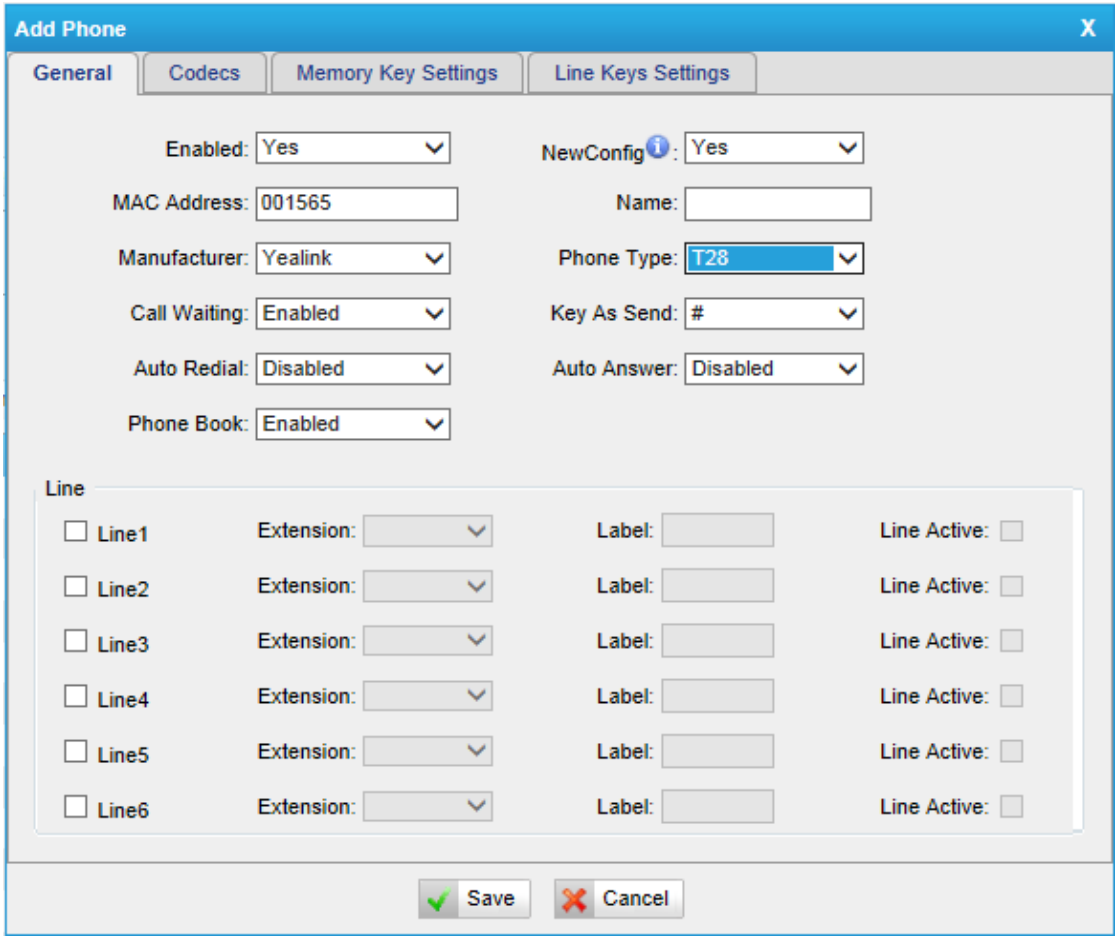


Figura 6-13

1) General

·Habilita
Seleccione sí o no para habilitar o deshabilitar esta extensión.

·Configuración Nueva
Si la versión del firmware del teléfono IP es superior a x.70.xx, debe seleccionar "Sí". O de lo contrario, debería ser "No".

·Dirección MAC
Introducir la dirección MAC del teléfono IP.

·Nombre
Pone el nombre de este teléfono aquí.

·Fabricante
Puede seleccionar el fabricante del teléfono IP.

·Tipo del Teléfono
Seleccione el modelo de su teléfono. Solamente para teléfono Snom

·Llamada en Espera
Esta función de llamada permite que su teléfono para aceptar otras llamadas entrantes a una extensión ya está en una llamada activa.

·Tecla como Envío
Configura una tecla como la de envío, y puede seleccionar #, * o deshabilitar esta función.

·Remarcación Automática
Habilita o deshabilita remarcación automática para el teléfono IP.

·Contesta Automática
Habilita o deshabilita contesta automática para el teléfono IP.

·Directorio Telefónico
Habilita o deshabilita esta función del directorio telefónico para el teléfono IP.

·Línea
Puede establecer cada línea del teléfono IP para la cuenta que quiere, activar o no.
Extensión: El número de la extensión seleccionado para el teléfono IP.
Discográfica: Se muestra en LCD para los usuarios a identificar la cuenta.
Línea Activa: Puede elegir on/off para activar / desactivar la cuenta respectivamente.

2) Códigos

En esta página, podemos establecer los códigos para el teléfono IP.

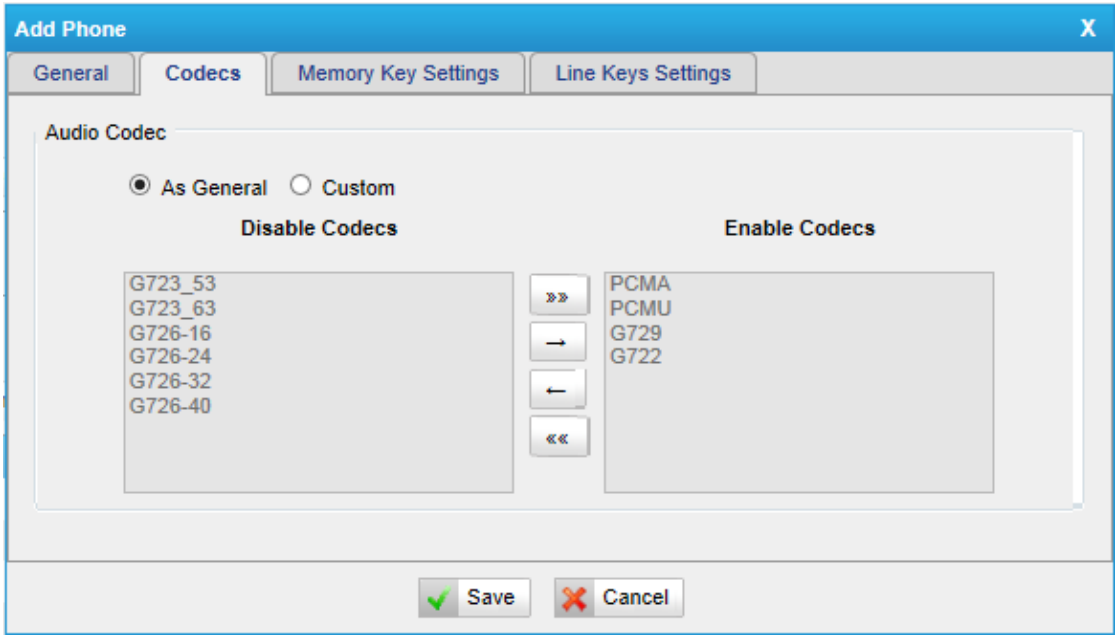


Figura 6-14

3) Configuraciones de Clave de Memoria

En esta página, podemos configurar claves DSS del teléfono IP uno por uno.

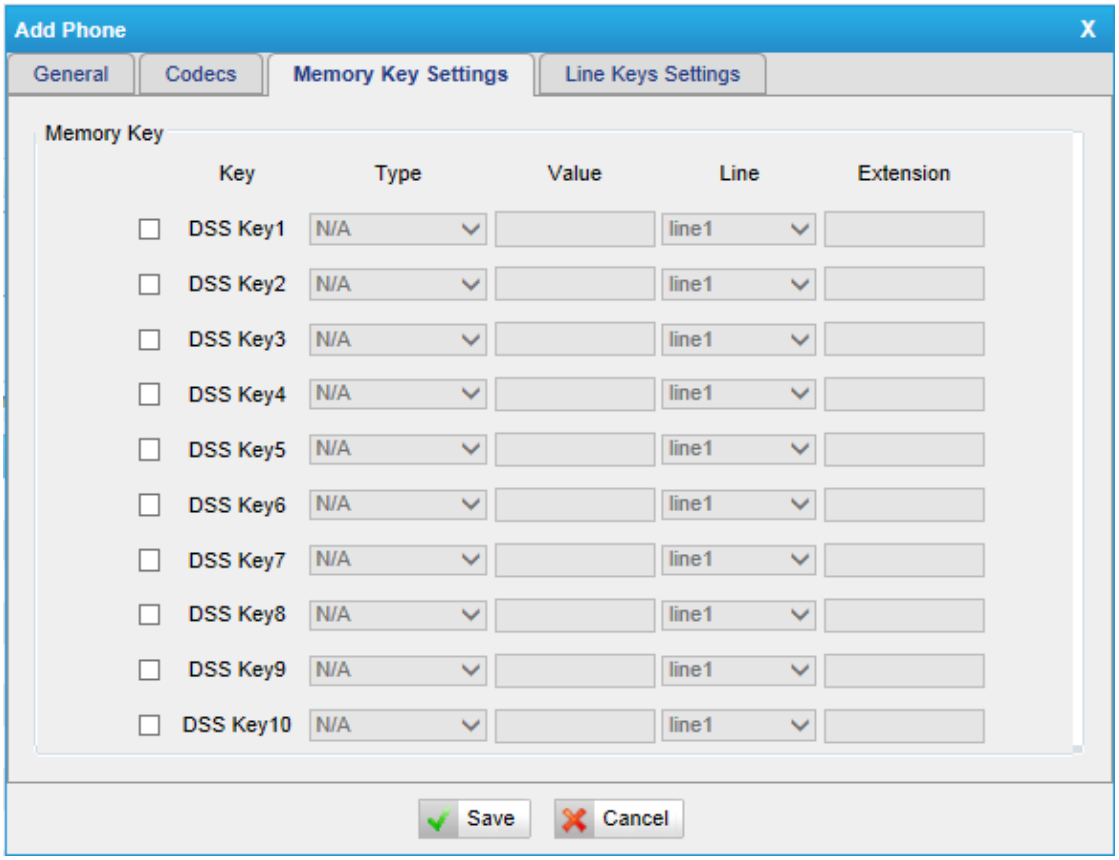


Figura 6-15

4) Configuraciones de Claves de Línea

Podemos configurar la clave de línea para este teléfono IP.

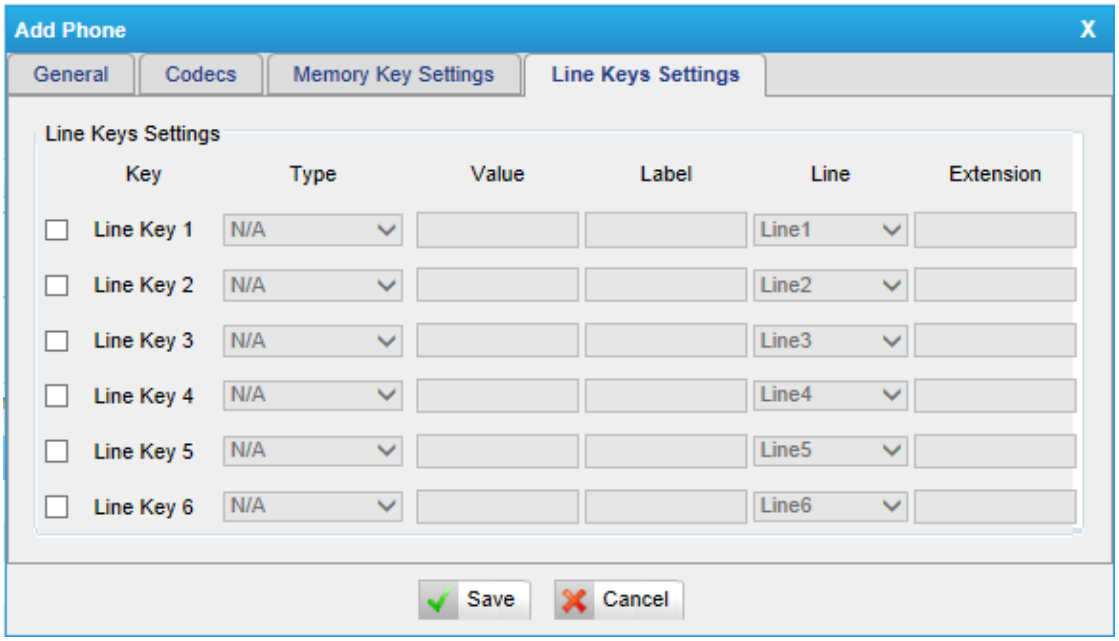


Figura 6-16

6.1.2.4 Teléfono no configurado

En esta sección, UNI-K escaneará todos los teléfonos soportados y se los mostrará aquí. Podemos hacer clic en "Dirección MAC" de un teléfono IP e introducir la información correspondiente en la ventana emergente, tal como figura 6-13.

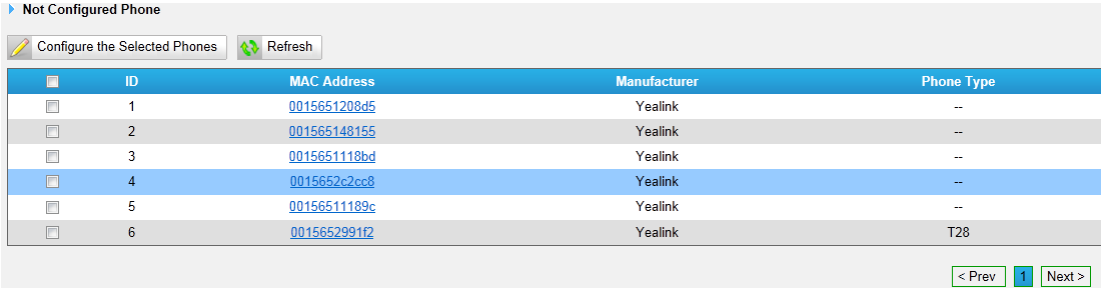


Figura 6-17

6.1.2.5 Cargar un Archivo

Haga clic en "Cargar un Archivo" y selecciona el archivo de configuración del teléfono IP en la ventana emergente.

Nota: El formato del archivo debe ser

Yealink: archivo de .cfg

Snom: archivo de .htm

Grandstream: archivo de .xml

Por favor editar los archivos de configuración con anticipación antes de la carga.

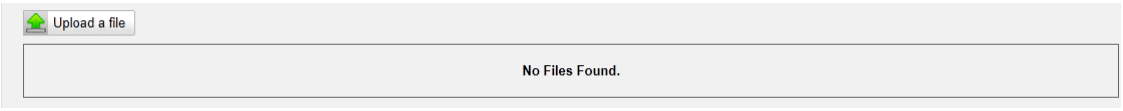


Figura 6-18

6.2 Troncales

6.2.1 Troncal Físico

Troncales múltiples son soportados en UNI-K IP PBX SC-32 V5, como BRI, PSTN. Por favor asegure que tiene los módulos instalados dentro antes del utilizar el troncal físico relacionado. Troncal BRI necesite módulo B2, y troncal PSTN necesite módulo O2.

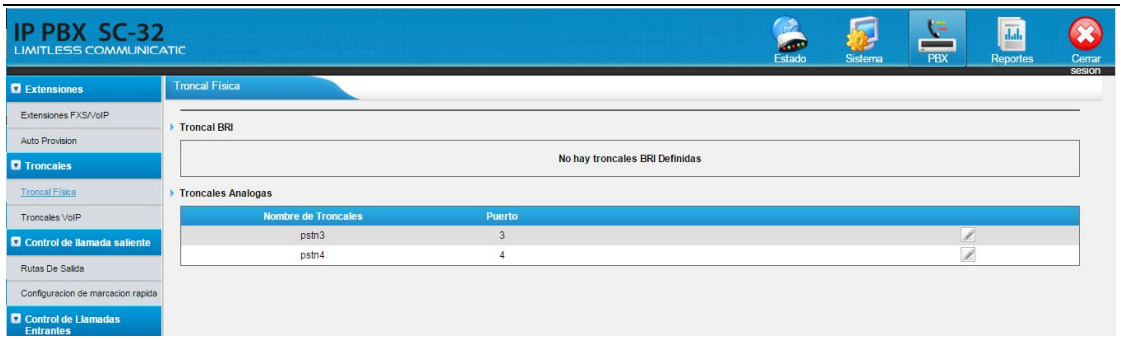


Figura 6-19

Troncal BRI

Interfaz de Tarifa Básica (BRI, 2B+D, 2B1D) es una configuración de red digital de servicios integrados (ISDN) destinados principalmente para uso en líneas abonadas similares a los que han sido utilizados para el servicio telefónico ordinario. La configuración BRI ofrece 2 canales portadores (canales B) en 64 kbit/s cada uno y un canal de datos (canal D) en 16 kbit/s. Los canales B se utilizan para voz o datos de usuarios, y el canal D se utiliza para cualquier combinación de datos, control/señalización, y las redes de paquetes X.25

Figura 6-20

Haga clic en editar para configurar los detalles de troncales BRI

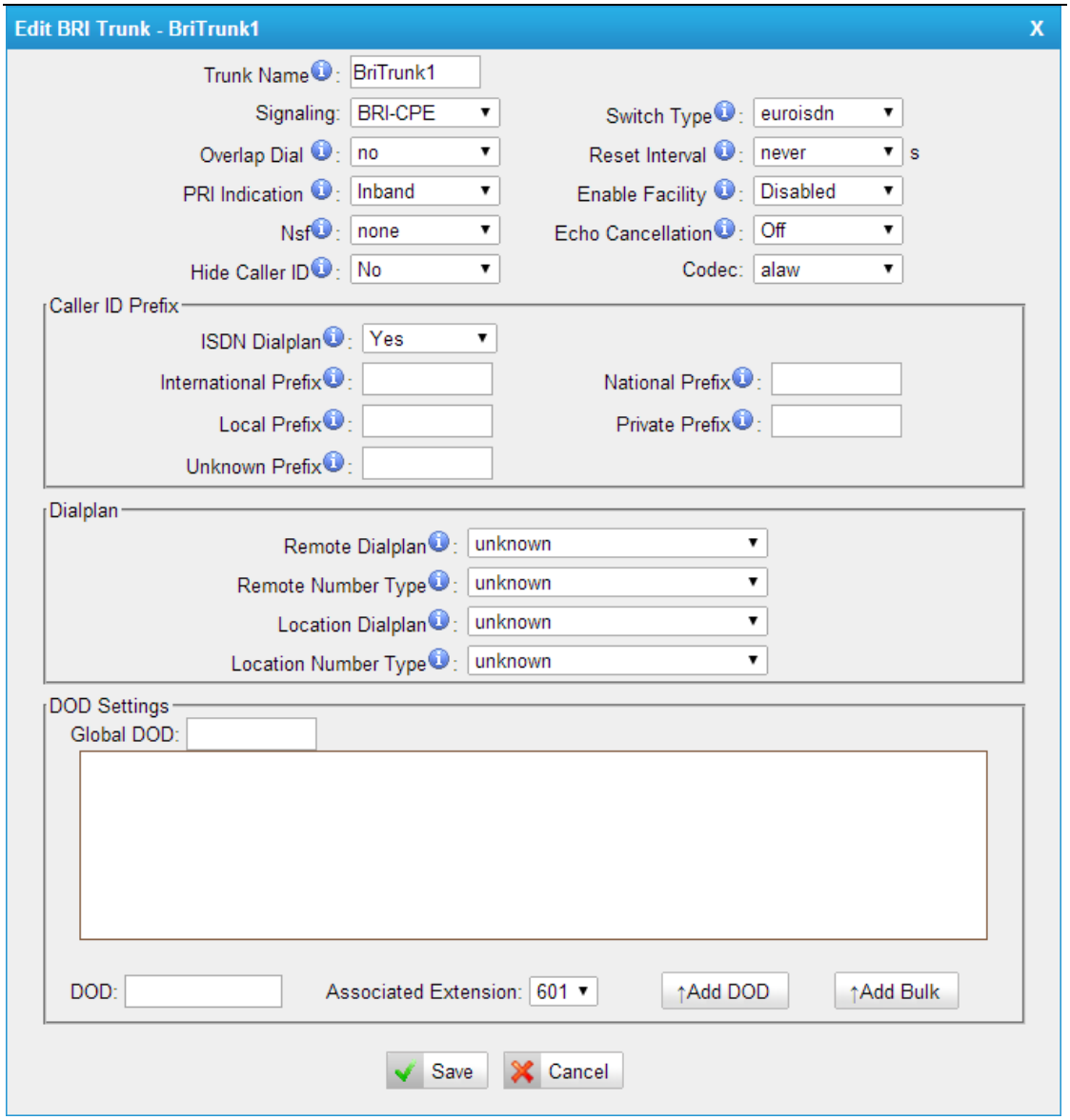


Figura 6-21

·Nombre de Troncal

Una etiqueta única utilizada para identificar este troncal cuando conste en reglas salientes, reglas entrantes, etc. Por ejemplo, "BriTrunk1".

·Señalización

Método de Señalización

BRI-CPE: ISDN BRI en modo TE y Punto a Punto.

BRI-CPE-PTMP: ISDN BRI en modo TE y Punto a Punto múltiple.

BRI-NET: ISDN BRI en modo NET y Punto a Punto.

BRI-NET-PTMP: ISDN BRI en modo NET y Punto a Punto múltiple.

·Tipo de conmutador

Nacional: ISDN nacional tipo2 (común en USA)

ni1: ISDN nacional tipo1

dms100: Nortel DMS100
4ess: AT&T 4ESS
5ess: Lucent 5ESS
euroisdn: EuroISDN
qsig: Protocolo de señalización de D-canal en punto de referencia Q para creación de red PBX.

·Marcación Superposición
Define si UNI-K puede marcar este conmutador utilizando los dígitos de superposición o no. Si necesita acceso telefónico en directo (DDI; en alemán "Durchwahl"), debe cambiar esto para sí, entonces UNI-K esperará después de que el último dígito que recibe.

·Restablecer intervalo
Ajuste el tiempo en segundos entre reanudación de los canales no utilizados. Algunas centrales no les gusta reiniciar los canales. Entonces establece el intervalo a un intervalo muy largo por ejemplo 100000000 o "nunca" a desactivar completamente. Si está en Israel, los siguientes son importantes: Como Bezeq en Israel no le gusta el B-Channel restablece sucediendo en las líneas, lo mejor es establecer el intervalo de reinicio en "nunca" cuando se instala una unidad en Israel. Nuestra experiencia pasada muestra también que este parámetro también puede causar problemas en los conmutadores locales en el UK y China.

·Indicación PRI
Avise el dispositivo cómo debe indicar Ocupado () y Congestión () para el conmutador / usuario. Los valores aceptados son:
Entrante: Dispositivo reproduce tonos de indicación sin contestar; no está disponible en todas las líneas de suscripción PRI / BRI.
Saliente: Dispositivo se desconecta con el código de información de ocupado / congestión manera que el conmutador se reproducirán los tonos de indicación a la persona quien llama. Ocupado () ahora hace lo mismo que establecer PRI_CAUSE = 17 y Colgar ().

·Habilitar Facilidad
Para habilitar la transmisión de servicios suplementarios ISDN basados en facilidad (tales como nombre del remitente de facilidad CPE más).

·NSF
Usado con AT&T PRIs. Si las llamadas salientes están siendo rechazadas debido al "elemento de información obligatorio ausente" y la IE falta es 0x20, entonces usted necesita este ajuste.

·Cancelación de Eco
Desactiva o activa la cancelación de eco;se recomienda que no desactivarla.

• Ocultar ID el Llamador
Si quiere otros usuarios ver su CID, por favor desactive esta opción.

·Código
Puede seleccionar alaw o ulaw.

1) Prefijo de ID de Llamada

·ISDN Plan de Marcación
Estas configuraciones se ponen a hacer ID prefijo trabaja conforme a la información enviada desde el proveedor de E1. Plan de numeración telefónica ISDN se recomienda E.164.

·Internacional Prefijo
Cuando hay llamadas internacionales entrando vía troncal BRI, el internacional prefijo establecido aquí agregará antes de CID. Así que puede saber esta es una llamada internacional antes de contestarla.

·Nacional Prefijo
Cuando hay llamadas nacionales entrando vía troncal BRI, el nacional prefijo establecido aquí agregará antes de CID. Así que puede saber esta es una llamada nacional antes de contestarla.

·Local Prefijo
Cuando hay llamadas locales entrando vía troncal BRI, el Local prefijo establecido aquí agregará antes de CID. Así que puede saber esta es una llamada local antes de contestarla.

·Privado Prefijo
Cuando hay llamadas privadas entrando vía troncal BRI, el Privado prefijo establecido aquí agregará antes de CID. Así que puede saber esta es una llamada privada antes de contestarla.

·Desconocido Prefijo
Cuando hay llamadas con número desconocido entrando vía troncal BRI, el desconocido prefijo establecido aquí mostrará como ID de llamada.

2) Plan de Marcación

·Plan de Marcación Remoto

Tipo de número de llamada

·Tipo de Número Remoto
Identificación de número de llamada

·Plan de Marcación Locación
Tipo de número de llamada

·Tipo de Número Locación
Identificación de número de llamada

3) Configuración DOD
·DOD Global
Marca número global de llamada saliente directamente

·DOD
Marca número de llamada saliente directamente
·Extensión Asociada
La extensión hace la llamada saliente vía troncal BRI mostrará DOD asociado.

·Añadir DOD
Añadir DOD para una extensión asociada.

·Añadir DOD Granel

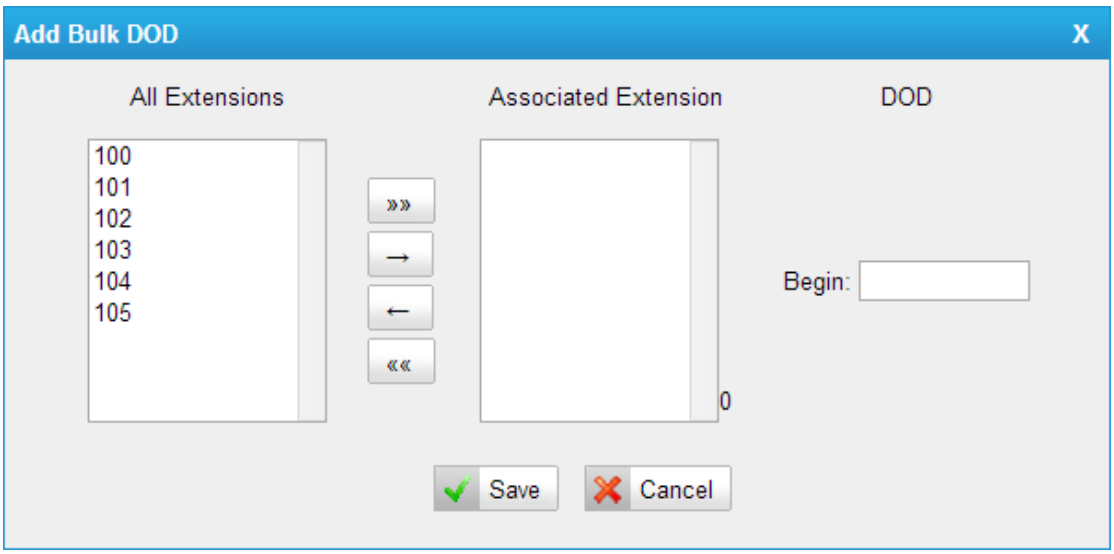


Figura 6-22

Añadir DOD granel para las extensiones a granel en secuencia ascendente con el "DOD Inicio" rellenado. Por ejemplo, si las Extensiones asociadas son 100, 101,

102, 103, 104, 105 con "DOD Inicio" es como 5500100, el DOD correspondiente serán 5500100, 5500101, 5500102, 5500103, 5500104, y 5500105.

Troncal PSTN

The public switched telephone network (PSTN) es una red pública mundial de la red telefónica de conmutación circuita.

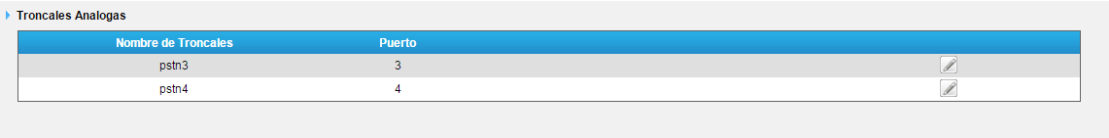


Figura 6-23

Haga clic en editar a configurar más detalles.

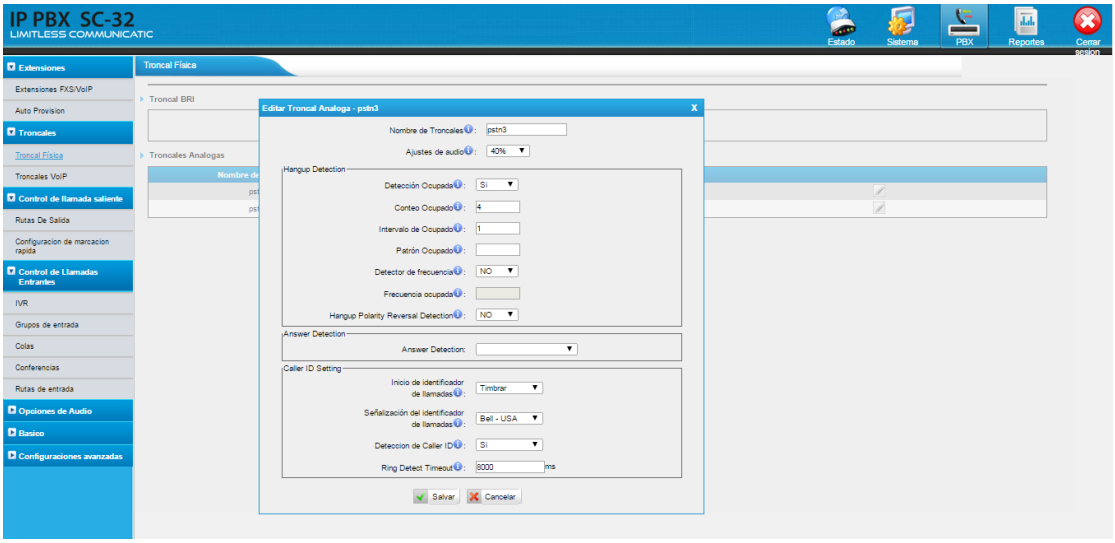


Figura 6-24

·Nombre de Troncal

Una etiqueta única utilizada para identificar este troncal cuando conste en reglas salientes, reglas entrantes, etc. Por ejemplo, "pstn5".

·Configuración de Volumen

Utilizado pra modificar el nivel del volumen de este troncal. Normalmente, esta

configuración no es necesaria a ser cambiada.

1) Detección de Hangup

·Detección de Ocupado

Detección de ocupado es utilizada para detectar otro extremo de colgar o para detectar una señal de ocupado. Selecciona "sí" para activar esta función.

·Contador de Ocupado

Si la detección de ocupado está activada, también es posible especificar el número de troncales ocupados en esperar antes de desconectar la llamada. El predeterminado es 4, pero los mejores resultados se pueda lograr si se establece en 6 o incluso 8. Recuerde que cuando mayor sea el número, se requerirá más tiempo para lanzar un canal. Un valor más alto reduce la probabilidad de que se encontrará al azar obsesiones.

·Intervalo ocupado

El intervalo de detección de ocupado

·Patrón Ocupado

Si la detección de ocupado está activada, también es posible especificar la cadencia de la señal de ocupado. En muchos países, es 500 mseg encendido, 500 ms apagado. Sin Patrón Ocupado especificado, UNI-K aceptará algún patrón regular sonido-silencio que repite las veces de <Contador de Ocupado> como una señal ocupada. Si especifica Patrón Ocupado, luego UNI-K comprobará además la duración del tono y el silencio, lo que reducirá aún más la posibilidad de una desconexión de falsos positivos.

·Detección de Frecuencia

Se utiliza para la Detección de Frecuencia (Habilitar la detección de la frecuencia de la señal ocupada o no).

·Frecuencia Ocupada

Si la Detección de Frecuencia está activada, deberá especificar la frecuencia local.

·Detección del Colgado de Inversión de Polaridad

La llamada será considerada como "colgada" en una inversión de la polaridad.

2) Detección de respuesta

·Detección de Respuesta

Configuración de Detección de Respuesta son configuradas para la tarifación exacta. Si el troncal PSTN envía la polaridad después de contestar la llamada, los usuarios pueden seleccionar "Detección de Polaridad"; o seleccionar

"Detección de Timbre" también, y establecen los detalles de las configuraciones correspondiendo al tono del timbre de la línea PSTN.

3) Configuración de ID de Llamada

·Iniciar ID de Llamada

Esta opción les permiten a definir el inicio de la señal de ID de Llamada:
Timbre: Inicia en cuando un timbre es recibido (la señalización de ID de Llamada: Bell_USA, DTMF).
Polaridad: Inicia en cuando una inversión de polaridad es empezada (la señalización de ID de Llamada: V23_UK, V23_JP, DTMF).
Antes de timbre: Inicia antes de un timbre es recibido (la señalización de ID de Llamada: DTMF).

·Señalización de ID de Llamada

Esta opción define el tipo de la señalización de ID de Llamada por utilizar. Puede establecer uno de los siguientes:
Bell: bell202 como utilizando en E.E.U.U.
v23_UK: adecuado en UK
v23_Japan: adecuado en Japón
v23-Japan pure: adecuado en Japón
DTMF: adecuado en Dinamarca, Suecia y Holanda

.Detección de ID de Llamada

Para troncales FXO, esta opción obliga a UNI-K aclarar ID de Llamada de las llamadas entrantes.

6.2.2 Troncal VoIP

Hay dos tipos de troncal VoIP en UNI-K U5XX: SIP y IAX, en esta página, podemos también configurar el troncal de “Proveedor de Servicio” , que no necesitan el nombre de uso y contraseña para la autorización, cuando ha comprado un troncal desde el proveedor con la dirección IP sólo, por favor seleccione el troncal de “Proveedor de Servicio”.

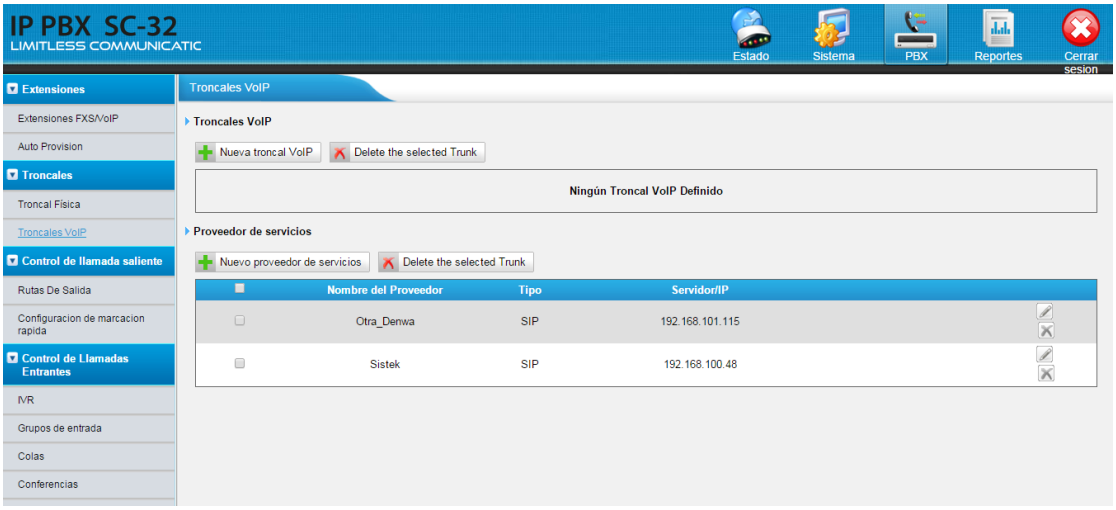


Figura 6-25

6.2.2.1 Troncal VoIP

En esta página, podemos configurar el troncal VoIP (SIP/IAX) que ha comprado desde el proveedor con la autorización del nombre y contraseña.

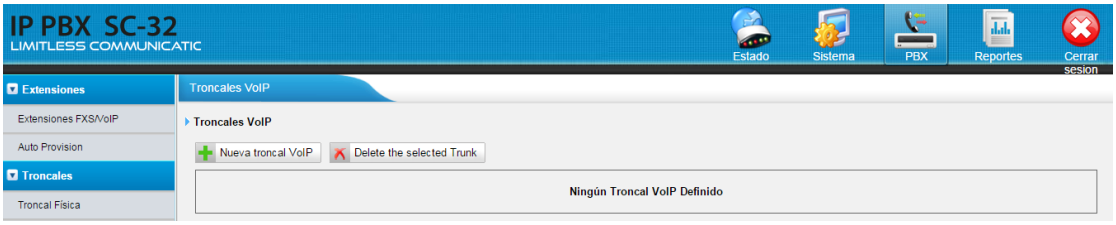


Figura 6-26

1) Añadir Troncal VoIP

Introduzca la información de SIP correcta (proporcionada por el proveedor VoIP). La información inexacta impedirá el tronco de registrarse. Puede eliminar troncales múltiples a la vez si es necesario.

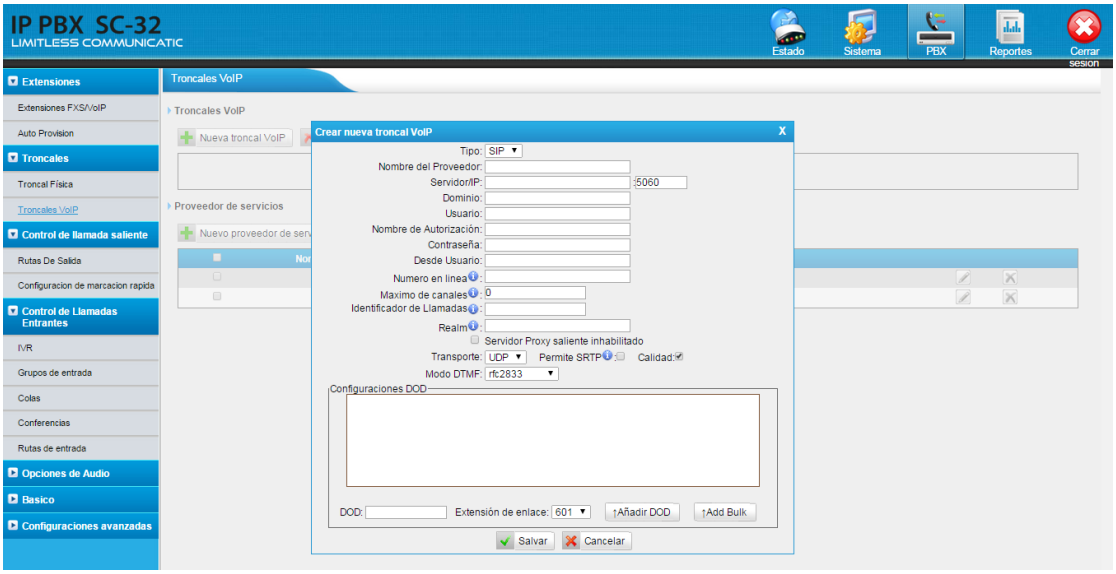


Figura 6-27

·Tipo
SIP – Identifique si el troncal envía y recibe llamadas utilizando el protocolo SIP de VoIP o no.

·Nombre del Proveedor
Una etiqueta única utilizada para identificar este troncal cuando conste en reglas salientes, reglas entrantes, etc. Por ejemplo, "SISTEK".

·Hostname/IP
El hostname o la dirección IP del proveedor del servicio. 5060 es el número de puerto estándar utilizado por el protocolo SIP. No cambie esta parte si no es obligatorio.

.Domain
El domain nombre del proveedor del servicio VoIP.

Nombre de Usuario
Nombre de Usuario de la cuenta SIP. Utilizado para la registración del troncal SIP.

.Autorización del nombre
Utilizado para la autentificación de SIP. Dejase en blanco si no lo requiere.

·Contraseña
Contraseña de la cuenta SIP.

.Desde Usuario
Todas las llamadas salientes desde este troncal SIP utilizarán Desde Usuario (en este caso el nombre de la cuenta para la registración de SIP) en Desde cabeza del paquete de invita del SIP. Dejase este campo en blanco si no lo necesite.

.Número en Línea
Define el número en línea que expectido por “conecta Skype” y algún otro proveedor de servicio SIP. Dejase este campo en blanco si no lo necesite.

·Canales Máximos
Controla el número máximo de canales salientes (llamadas simultaneas) que puede ser utilizado en este troncal. Llamadas entrantes no se contadas contra el máximo. Pone como 0 para especificar no máximo.

·Identificador de Llamada

Especifique el ID de llamada para utilizarse cuando haga las llamadas salientes a través de este troncal. El ID de llamada establecido en la página "Extensión" se anulará el ID de llamada establecido en la página de "Troncal VoIP" Contacta con su proveedor de servicios por más información. Contacta con su proveedor de servicio para más información.

·Servidor Proxy Saliente

Un proxy que recibe peticiones desde un cliente. A pesar de que puede no ser el servidor resuelto por el Request-URI.

·Realm

Realm es una cadena que se mostrará a los usuarios para que sepan qué nombre de usuario y la contraseña que desea utilizar.

·Códigos

Define el código para este troncal SIP y su prioridad.

Nota: Para cambiar el tipo de código y prioridad de este troncal, por favor, primero lo crea, que aparecerá cuando se edita de nuevo.

·Transporte

Este será el método de transporte utilizado por el Troncal SIP. Este método se ofrecido por el proveedor de troncal SIP. Estas opciones son UDP (Por defecto) o TCP o TLS.

·Habilita SRTP

Define si SRTP está habilitado para este troncal.

·Calificar

Enviar los paquetes de comprueba vivas al proveedor SIP.

·DTMF modo

Establece modo predeterminado para enviar DTMF of este troncal. Configuración predeterminada: rfc2833

·DOD

DOD (marcación directa) significa que el identificador de llamadas desaparece al marcar fuera. Antes de configurar este, por favor aseguren que el proveedor soporta esta función.

·Extensión Asociada

La extensión hace la llamada saliente vía troncal SIP mostrará DOD asociado.

·Añadir DOD

Añadir DOD para una extensión asociada.

·Añadir DOD Granel

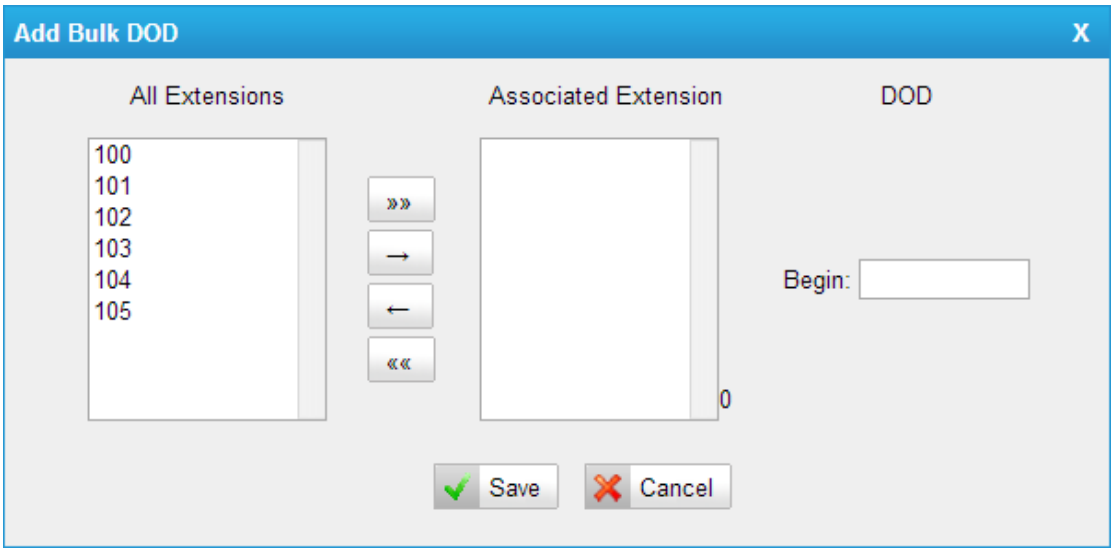


Figura 6-28

Añadir DOD granel para las extensiones a granel en secuencia ascendente con el "DOD Inicio" rellenado. Por ejemplo, si las Extensiones asociadas son 100, 101, 102, 103, 104, 105 con "DOD Inicio" es como 5500100, el DOD correspondiente serán 5500100, 5500101, 5500102, 5500103, 5500104, y 5500105.

2) Añadir Troncal IAX

Introduzca la información de IAX correcta (proporcionada por el proveedor VoIP). La información inexacta impedirá el tronco de registrarse.

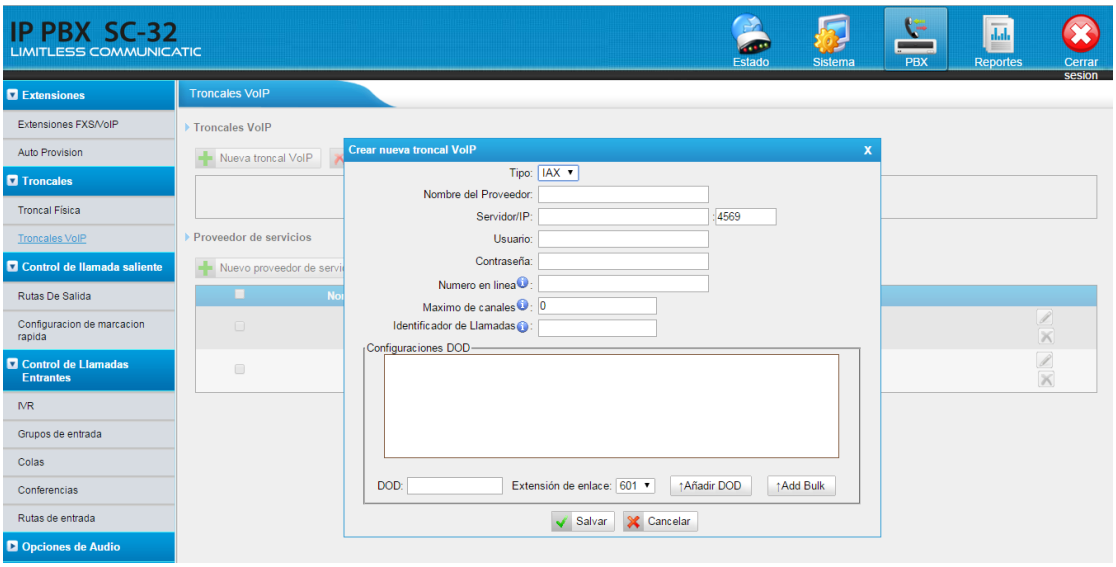


Figura 6-29

·Tipo
IAX – Identifique si el troncal envía y recibe llamadas utilizando el protocolo SIP de IAX.

·Nombre del Proveedor
Una etiqueta única utilizada para identificar este troncal cuando conste en reglas salientes, reglas entrantes, etc. Por ejemplo, "SISTEK2".

·Hostname/IP
Hostname o la dirección IP del proveedor del servicio. 4569 es el número puerto estandarizado utiliza por protocolo IAX. No cambie esta parte si no es obligatorio.

Nombre de Usuario
Nombre de Usuario de la cuenta IAX; utiliza por registro de troncal IAX.

·Contraseña
Contraseña de la cuenta IAX

.Número en Línea
Define el número en línea que expectido por "conecta Skype" y algún otro proveedor de servicio SIP. Dejase este campo en blanco si no lo necesite.

·Canales Máximos
Controla el número máximo de canales salientes (llamadas simultaneas) que puede ser utilizado en este troncal. Llamadas entrantes no se contadas contra el máximo. Pone como 0 para especificar no máximo.

·Identificador de Llamada
Especifique el ID de llamada para utilizarse cuando haga las llamadas salientes a través de este troncal. El ID de llamada establecido en la página "Extensión" se anulará la configuración del ID de llamada establecido en la página de "Troncal VoIP" Contacta con su proveedor de servicios por más información. Contacta con su proveedor de servicio para más información.

·DOD
DOD (marcación directa) significa que el identificador de llamadas desaparece al marcar fuera. Antes de configurar este, por favor aseguren que el proveedor soporta esta función.

·Extensión Asociada
La extensión hace la llamada saliente vía troncal IAX mostrará DOD asociado.

·Añadir DOD

Añadir DOD para una extensión asociada.

·Añadir DOD Granel

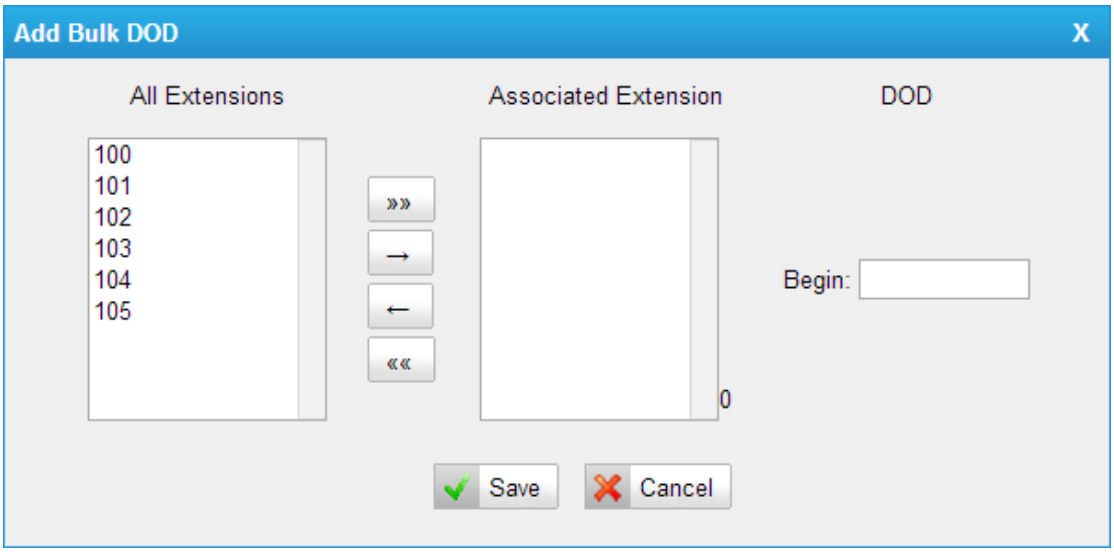


Figura 6-30

Añadir DOD granel para las extensiones a granel en secuencia ascendente con el "DOD Inicio" rellenado. Por ejemplo, si las Extensiones asociadas son 100, 101, 102, 103, 104, 105 con "DOD Inicio" es como 5500100, el DOD correspondiente serán 5500100, 5500101, 5500102, 5500103, 5500104, y 5500105.

6.2.2.2 Proveedor de Servicio

En esta página, podemos configurar el Proveedor del Servicio.

Puede agregar Proveedor del Servicio como requiere. Y también puede eliminar troncales múltiples a la vez por marcando la casilla de verificación según se requiera.

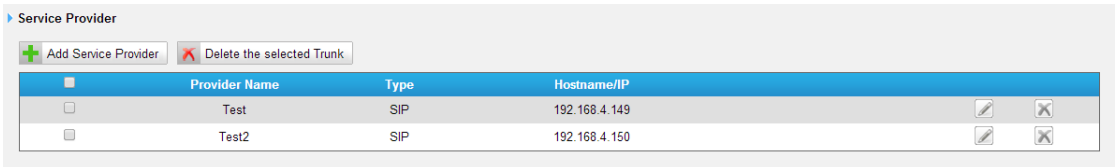


Figura 6-31

A continuación se muestra un troncal de Proveedor de servicios (punto a punto modo), que autoriza el uso de única dirección IP. Si usted tiene un troncal con una dirección IP sola, elija este tipo.

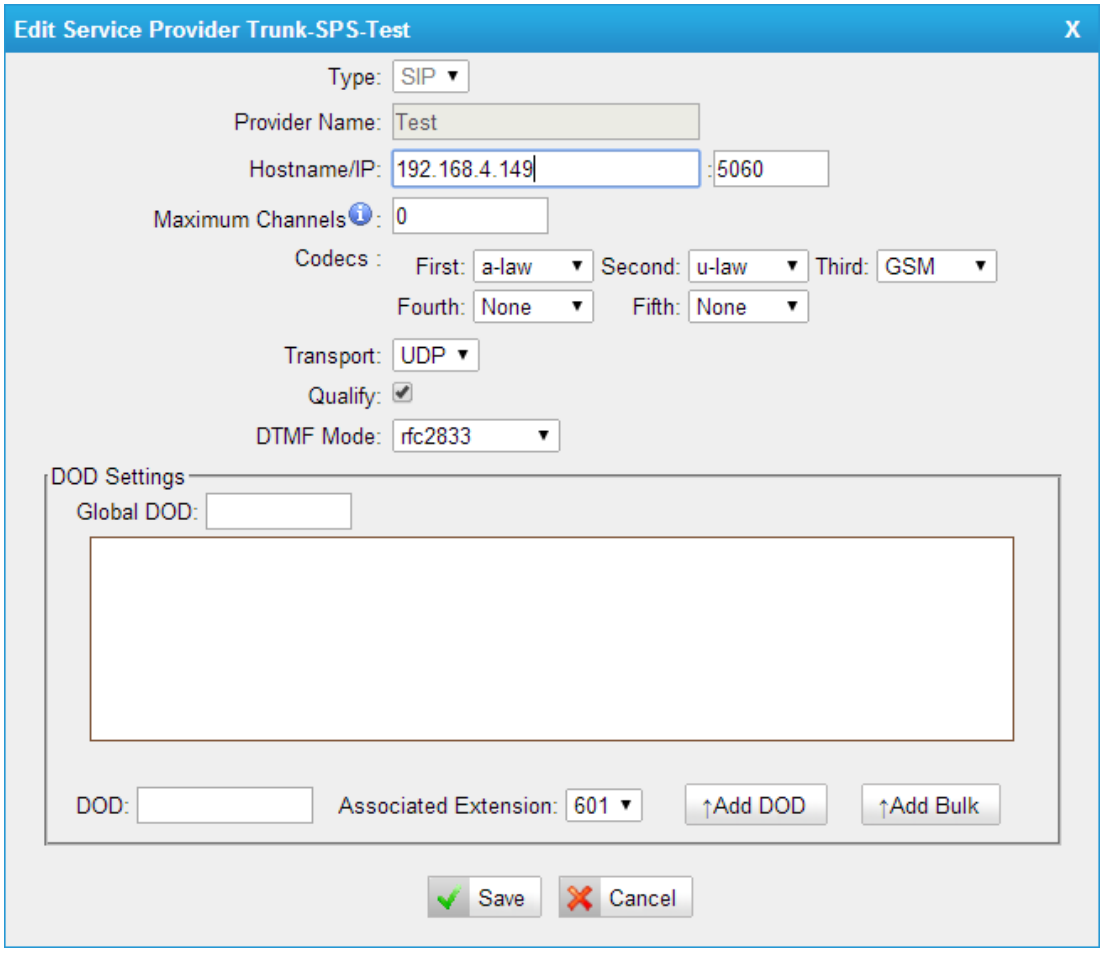


Figura 6-32

·Tipo

SIP o IAX

SIP – Identifique si el troncal envía y recibe llamadas utilizando el protocolo SIP de VoIP.

IAX – Identifique si el troncal envía y recibe llamadas utilizando el protocolo SIP de IAX.

·Nombre del Proveedor

Una etiqueta única ayudaría a identificar este troncal. Por ejemplo "Provider2".

·Hostname/IP

Hostname o la dirección IP del proveedor del servicio.

Nota: 5060 es el número de puerto estándar utilizado por el protocolo SIP, 4569 es el número de puerto estándar utilizado por el protocolo IAX. No cambie esta parte si no es obligatorio.

·Canales Máximos

Controla el número máximo de canales salientes (llamadas simultaneas) que puede ser utilizado en este troncal. Llamadas entrantes no se contadas contra el máximo. Dejar en blanco para especificar ningún máximo.

·Códigos

Define el código para este troncal SIP y su prioridad.

Nota: código sólo puede mostrarse cuando se edita después de la creación del troncal.

·Transporte

Este será el método de transporte utilizado por el Troncal SIP. Este método se ofrecido por el proveedor de troncal SIP. Estas opciones son UDP (Por defecto) o TCP o TLS.

·Calificar

Enviar los paquetes de comprueba vivas al proveedor SIP.

·DTMF modo

Establece modo predeterminado para enviar DTMF of este troncal. Configuración predeterminada: rfc2833

·DOD

DOD (marcación directa) significa que el identificador de llamadas desaparece al marcar fuera. Antes de configurar este, por favor aseguren que el proveedor soporta esta función.

·Extensión Asociada

La extensión hace la llamada saliente vía este troncal mostrará DOD asociado.

·Añadir DOD

Añadir DOD para una extensión asociada.

·Añadir DOD Granel

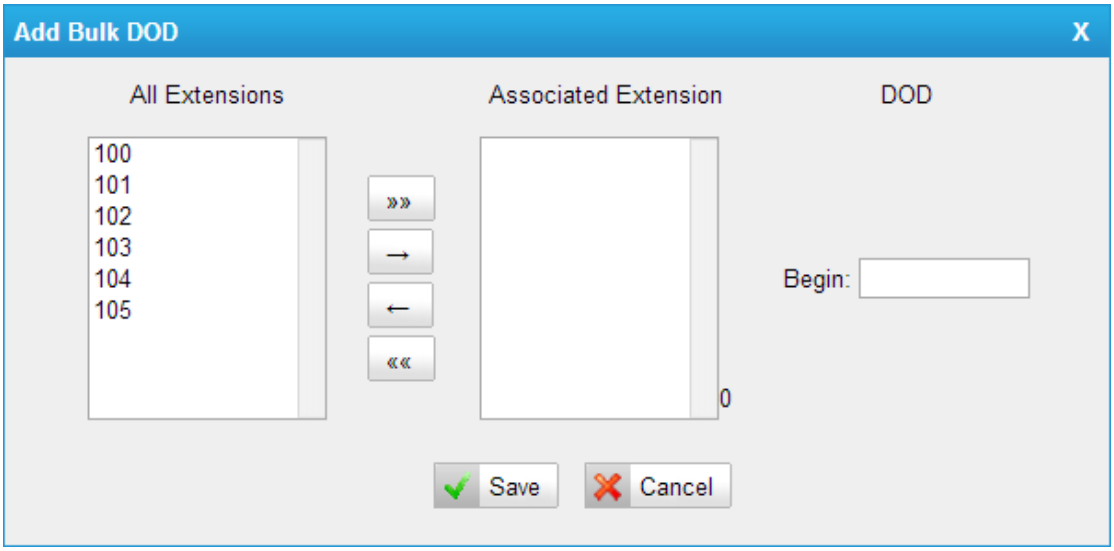


Figura 6-33

Añadir DOD granel para las extensiones a granel en secuencia ascendente con el "DOD Inicio" rellenado. Por ejemplo, si las Extensiones asociadas son 100, 101, 102, 103, 104, 105 con "DOD Inicio" es como 5500100, el DOD correspondiente serán 5500100, 5500101, 5500102, 5500103, 5500104, y 5500105.

6.3 Control de Llamada Saliente

6.3.1 Routes Salientes

En esta página, podemos configurar las reglas salientes para controlar las llamadas salientes.

Notas:

1. El número máximo de route saliente es 32.
2. Si los patrones de marcado son los mismos en varios routes, UNI-K elegirá los routes disponibles desde arriba hasta el último.
3. Cuando tiene una nueva extensión creada, por favor edite el route saliente para que pueda marcar hacia afuera también.

Figura 6-34

Podemos crear route saliente o utilizar el rote predeterminado “pstnout” (Marque 9+Números para hacer llamadas) Puede eliminar troncales salientes múltiples a la vez si es necesario.

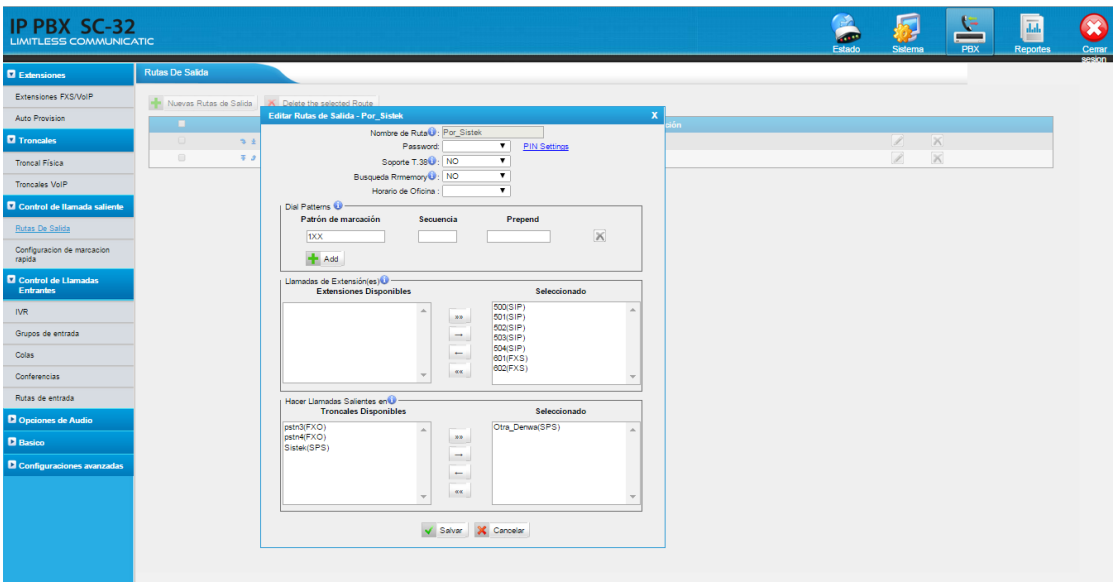


Figura 6-35

·Nombre de Route
Nombre de este Route Saliente. Por Ejemplo "Local" o "Larga Distancia".

·Contraseña
La contraseña del route puede ser utilizado para proteger este route desde el acceso sin una contraseña. Puede seleccionar una de las contraseñas en la lista PIN que puede hacer clic en "configuraciones PIN" para editarla en la página de "configuraciones PIN".

Soporta T.38:
Habilita Fax T.38 en este route saliente (sólo para el troncal SIP).

·Rrmemory Hunt
Circula por turno con memoria recuerda cuál troncal se utilizó la última vez, y luego utiliza el siguiente troncal disponible a llamar.

·Horarios Oficiales
Cuando un horario oficial especificado fue seleccionado, este route saliente puede solamente ser utilizado durante este horario oficial, y no puede ser utilizado afuera del horario oficial.

·Patrón de Marcado
Las llamadas salientes que coincide por este patrón utilizará este rote saliente. Hay un número del carácter del patrón de marcado que tiene significación especial:
X: Algún dígito desde 0-9
Z: Algún dígito desde 1-9
N: Algún dígito desde 2-9
[12345-9]: Algún dígito en ménsulas (en este ejemplo, 1,2, 3,4, 5,6, 7,8, 9)
El "**.**" El carácter coincidirá con todos los dígitos restantes. Por ejemplo, "9011." coincidirá algún número telefónico que empiece con "9011", incluyendo "9011" .
El "**!**" Coincidirá con ninguno dígitos restantes, y hace que el proceso de correspondencia para completar lo antes que se pueda determinar que no hay otros partidos son posibles.

Ejemplo 1: **NXXXXXX** coincidirá algún número telefónico de 7 dígitos.
Ejemplo 2: **1NXXNXXXXX** coincidirá un número telefónico empiece con 1, a continuación por 3 dígitos de área, y luego número de 6 dígitos.

·Tira
Permite al usuario especificar el número de dígitos que se despojaron de la parte delantera del número de teléfono antes de que se hiciera la llamada. Por

ejemplo, si los usuarios deben presionar 0 antes de marcar un número telefónico, un dígito debe ser despojado desde la cadena de marcación antes de que realizar la llamada.

·Anteponga

Estos dígitos antepondrá al número telefónico antes de realizar la llamada. Por ejemplo, si un troncal requiere una marcación de 10 dígitos, pero los usuarios son más cómodos con la marcación de 7 dígitos, este campo puede utilizarse a anteponer un código de área de 3 dígitos a todos los números telefónicos de 7 dígitos.

·Agregar

Agrega patrones de marcado múltiples en este route saliente.

·Miembros Extensiones

Define las extensiones que serán permitidas a utilizar este route saliente.

·Miembros Troncales

Define el troncal que pueda ser utilizado para este route saliente.

6.3.2 Configuraciones de Marcado Rápido

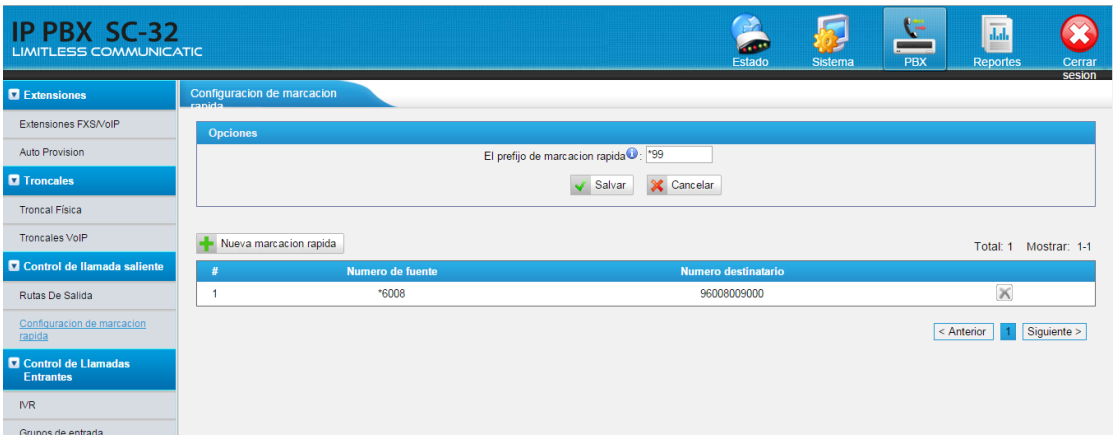


Figura 6-36

1) Opciones

·El prefijo de marcado rápido

El prefijo debe ser marcado antes del número de marcado rápido. El valor predeterminado es *99.

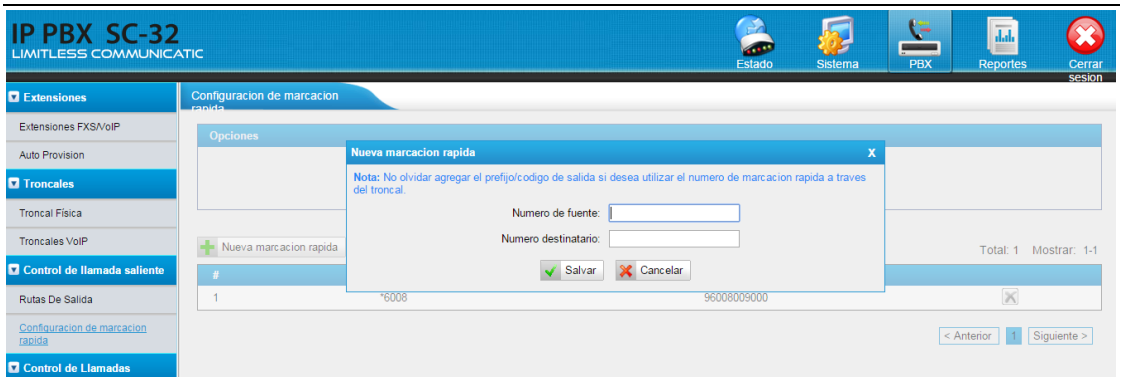


Figura 6-37

2) Agregar una marcado rápido nueva.

·Fuente de Número

El número de marcado rápido.

·Número de Destino

El número quiere llamar.

Por ejemplo la fuente e número es "123". El número de destino es "5503305". El número prefijo es "99". Puede utilizar una extensión con algún tipo a marcar *99123, luego llamará el número 5503305.

Nota: No se olvide a agregar una marcación saliente prefija si quiere marcar un número de marcación rápida a través el troncal.

6.4 Control de Llamada Entrante

En esta página, podemos configurar los detalles de IVR, grupo de timbre, cola y routes entrantes.

6.4.1 IVR

Cuando hay una llamada entrante apunta a la operadora automática, UNI-K reproducirá una grabación de IVR y rutará la llamada al destino solicitado (por ejemplo, "Bienvenido a la empresa XX, para ventas marque 1, para soporte técnico marque 2, para el operador marque 0 ", etc.). El sistema transferirá la llamada a la extensión correspondiente dependiendo los dígitos DTMF presionado por el usuario.

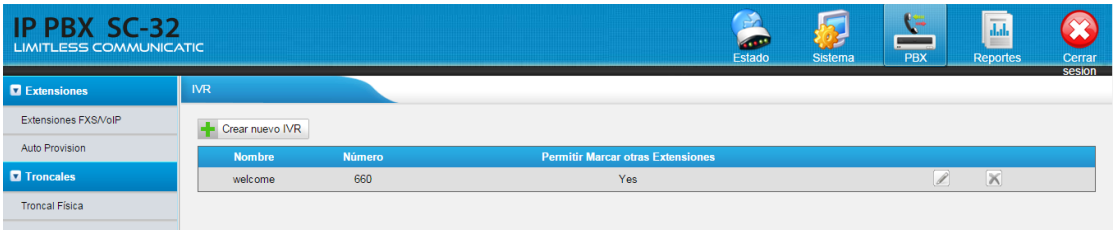


Figura 6-38

Hay un IVR por defecto aquí, podemos editarlo directamente o agregar IVR por sí mismo.

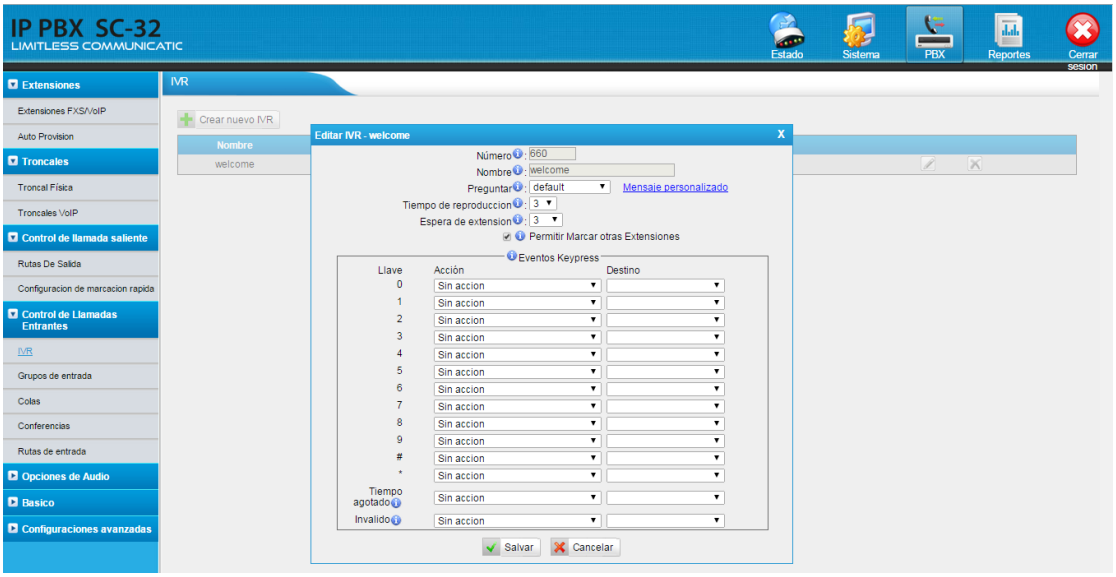


Figura 6-39

·Número

UNI-K trata IVR como una extensión; puede marcar el número de esta extensión para alcanzar este IVR desde las extensiones internas.

·Nombre

Un nombre para el IVR

·Aviso

El aviso grabado que reproducirá cuando se alcanza este IVR.

·Número de Repetición

El número de veces que reproducirá el aviso de IVR seleccionado.

·Tecla de Tiempo de Espera

Espera al usuario para entrar a una extensión nueva por un número especificado de segundos.

·Habilita la Marcación Directa
Permite el llamador a marcar números de otras extensiones directamente.

·Eventos de tecla presa
Una lista de las acciones que puede ser realizada dependiendo en el dígito marcado por el usuario.

·Tecla
La tecla pulsada cuando los llamadores escuchan el aviso del IVR.

·Acción
Cuando los llamadores presionen la tecla correspondiente, la acción que UNI-K la ejecutará.
Sin Acción: No hace nada
Conecta a extensión: Conecta la llamada a una extensión.
Conecta a Voicemail: conecta la llamada al voicemail de una extensión.
Conecta al Grupo de Timbre: Conecta la llamada a un grupo de timbre.
Conecta a IVR: Conecta la llamada a un IVR.
Conecta a la sala de Conferencia: Conecta la llamada a una sala de conferencia.
Conecta a DISA: Conecta la llamada a una DISA.
Conecta a la Cola: Conecta la llamada a una cola.
Conecta a Faxes: Conecta la llamada a faxes de las extensiones.
Marcar por Nombre: Los llamadores pueden marcar el nombre de una extensión para conectarse a la extensión correspondiente.
Colgado: Cuelga la llamada.

·Destinación
Donde UNI-K rutará la llamada cuando la acción ocurra.

·Tiempo de Espera
Define la acción del tiempo de espera Un tiempo de espera ocurre después de aviso de IVR ha determinado reproducción del número de veces especificado por el "Número de Repetición" campo.

·Inválido
Define la acción inválida. La acción inválida se activa si el usuario introduce un dígito DTMF que no está definida para este IVR.

6.4.2 Grupo de Timbre

Grupo de timbre se puede configurar para equilibrar el tráfico de llamadas para múltiples usuarios y dar las personas que llaman un mayor nivel de disponibilidad para las llamadas entrantes. Métodos de timbres múltiples y voicemail son soportados.

Nota: la función de follow me en la página de extensión no tendrá efecto cuando está sonando como un agente.

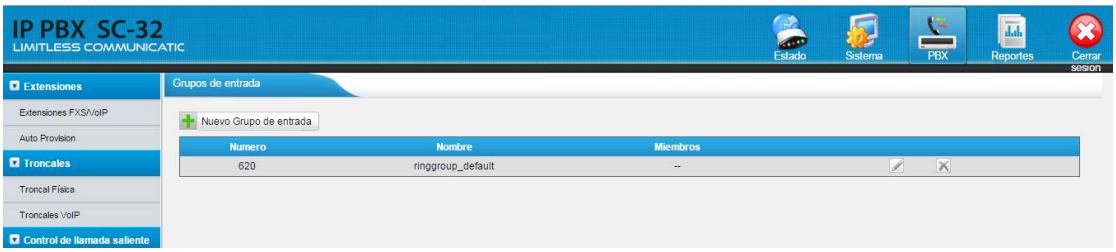


Figura 6-40

Hay un grupo de timbre por defecto, puede editarlo o crear un nuevo.

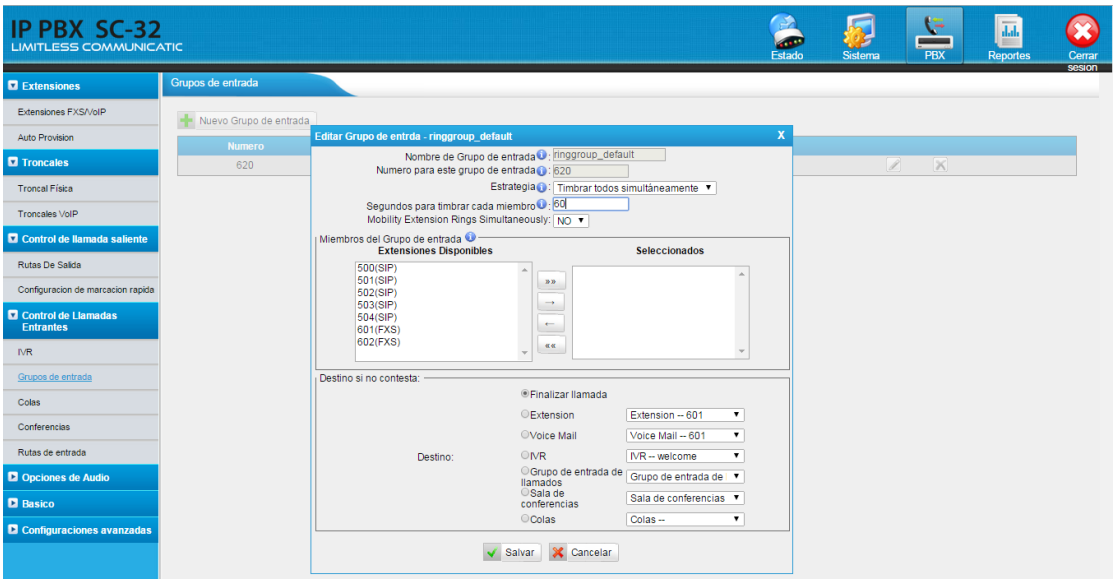


Figura 6-41

·Nombre del Grupo de Timbre

Esta opción define un nombre para este grupo, por ejemplo "Ventas". "Nombre del Grupo de Timbre" es una etiqueta para ayudarle a identificar este grupo en la lista de grupos.

·Número del Grupo de Timbre

Esta opción define el número de extensión que puede ser marcado para alcanzar este grupo.

·Estrategia

Esta opción establece la Estrategia de timbre para este grupo. Las opciones son como las siguientes:

1. Suenan todos simultáneamente: Suenan todas las extensiones disponibles simultáneamente.
2. Suenan secuencialmente: Suena cada extensión in el grupo una en un tiempo.

·Extensión de Movilidad Suena Simultáneamente

Si se establece en sí, cuando la extensión en el grupo de Timbre es llamada, la extensión de movilidad asociada sonará simultáneamente. De antemano, la opción de "Suena simultáneamente" se debe marcar en la configuración de extensiones.

·Segundos para que suene cada miembro

1. Si la estrategia es "Suena Todo simultáneamente", significa que el número de segundos para que suene este grupo antes de rutar la llamada de acuerdo con la configuración de "Destino si no hay respuesta".
2. Si la estrategia es "Suena secuencialmente", significa que el número de segundos para que suene una extensión sola antes de moverse a la próxima.

·Miembros del Grupo de Timbre

Una extensión puede hacerse miembro de este grupo de timbre moviendo en el cuadro "Seleccionado".

·Destino Si No Hay Respuesta

Cuando todos los miembros en este grupo fallan a contestar la llamada, el sistema pasará la llamada correspondiendo al destino seleccionado.

6.4.3 Cola

Cola de Llamada ofrece los usuarios (por ejemplo call centers) un medio eficiente para tener sus llamadas atendidas en la orden en que se recibieron para ofrecer un servicio superior al cliente de nivel.

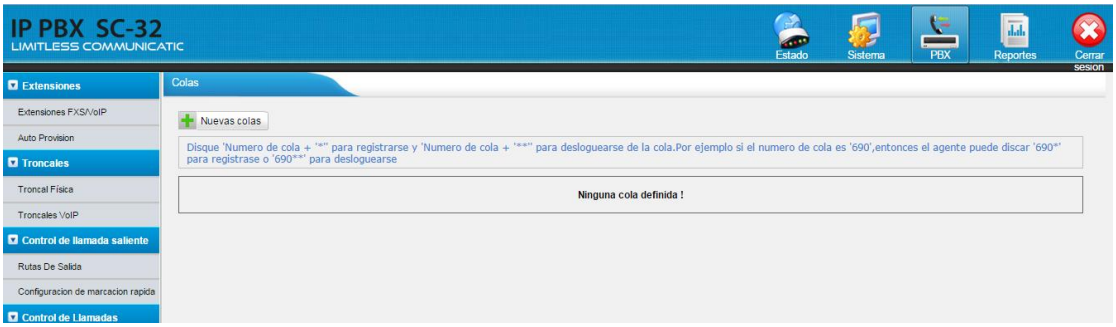


Figura 6-42

Cola de llamada permite que las llamadas sean secuenciadas para uno o más agentes.

Notas:

1. Marcar "número cola + '*'" loqueado o "número de cola + '**'" para salir de la cola. Por ejemplo, si el número de la cola es “680”, luego el agente puede marcar “680” para ingresarse o “680**” para salir.
2. La función de follow me en la página de extensión no tendrá efecto cuando está sonando como un agente de la cola.

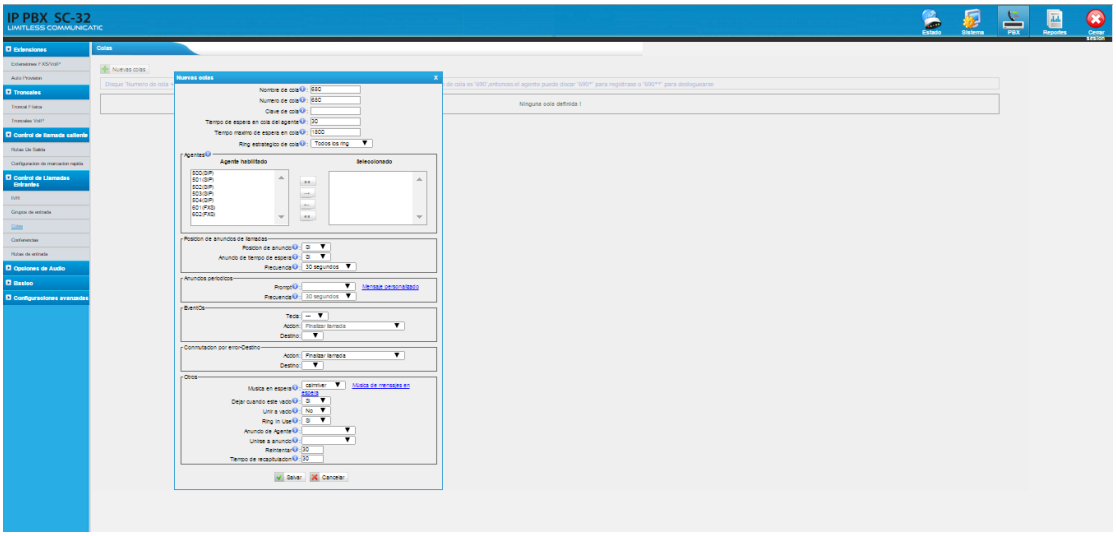


Figura 6-43

·Nombre de la Cola

Un nombre para la Cola

·Número de la Cola

Utiliza el número para marcar a la cola, o transferir llamadores a este número

para que dejar a esta cola.

·Contraseña de la Cola
Puede requerir agentes a ingresar una contraseña antes de poder entrar esta cola.

·Tiempo de Espera de Agente de Cola
El número de segundos del teléfono de un agente puede sonar antes de lo consideramos un tiempo de espera.

·Tiempo de Espera Máximo de la Cola
El número de segundos máximo que un llamador puede esperar en la cola antes de ser retirado(0 para ilimitado).

·Estrategia de Timbre de la Cola
Esta opción establece la Estrategia de timbre para esta Cola. Las opciones son
Suena Todo: Suenan todos Agentes disponibles simultáneamente hasta uno la contesta.
Salir Recientemente: Suena el Agente que salió recientemente de llamada.
Llamadas Menores: Suena el Agente con las llamadas completadas menores.
Aleatorio: Suena a un Agente aleatorio.
Turno Rondo con Memoria: Turno Rondo con Memoria, recuerda donde lo dejó en el último sonido pasaron.

1) Agentes
Esta selección muestra a todos los usuarios. Selecciona un usuario aquí, le hace un agente de la cola actual.

2) Anuncios de la Posición de llamador
Anuncia Posición
Anuncia posición de llamador en la cola.

·Anuncia tiempo en Espera
Habilita esta opción causará UNI-K a anunciar el tiempo en espera al llamador periódicamente basado en el temporizador de frecuencia. Sí o no; tiempo de retención no se dará a conocer si <1 minuto.

·Frecuencia
La frecuencia a anunciar la posición en cola y tiempo en espera estimado.
Nota: "0 segundo" significa desactiva el anuncio.
3) Anuncios Periódicos
·Aviso
Selecciona un archivo de aviso para reproducir periódicamente.

·Frecuencia
La frecuencia a anunciar un aviso para el llamador.

4) Eventos
Si un llamador marca la tecla cuando está esperando en la cola, esta configuración seleccionará cuál acción procesará la tecla marcada.

5) Conmutación por error-Destino
Define la acción de Conmutación por error. Una conmutación por error ocurra después del usuario llega el tiempo máximo de espera en la cola.

6) Otras
· Música en Espera
selecciona la clase de "Música en Espera" para esta cola.

·Dejar cuando Vacío
Esta opción controla si los llamadores ya en espera son forzados a salir de una cola que no tiene agentes. Hay dos opciones.
Sí: Los llamadores son forzados a salirse de una cola cuando no hay agentes ingresados.
No: Los llamadores mantienen en una cola sin agentes.

·Unir Vacío
Esta opción controla si los llamadores pueden unirse una cola de llamada que no hay agentes o no. Hay dos opciones.
Sí: Los llamadores puede unirse una cola de llamada sin agentes o solo agentes no disponibles.
No: Los llamadores no pueden ingresar una cola en cuando no hay agente en la cola.
La opción por defecto es no.

·Anuncio de Agente
Anuncio reproduce al Agente antes del unirse con los llamadores.

·Unir Anuncio
Anuncio reproduce a los llamadores antes de unirse con la cola.

·Reintentar
El número de segundos podemos esperar antes de intentar todos teléfonos otra vez.

·Recapitula tiempo

Cuantos segundos después de la terminación de una llamada que una Agente tendrá antes de la cola que les suena una llamada nueva. Es 30 segundos por defecto.

6.4.4 Conferencias

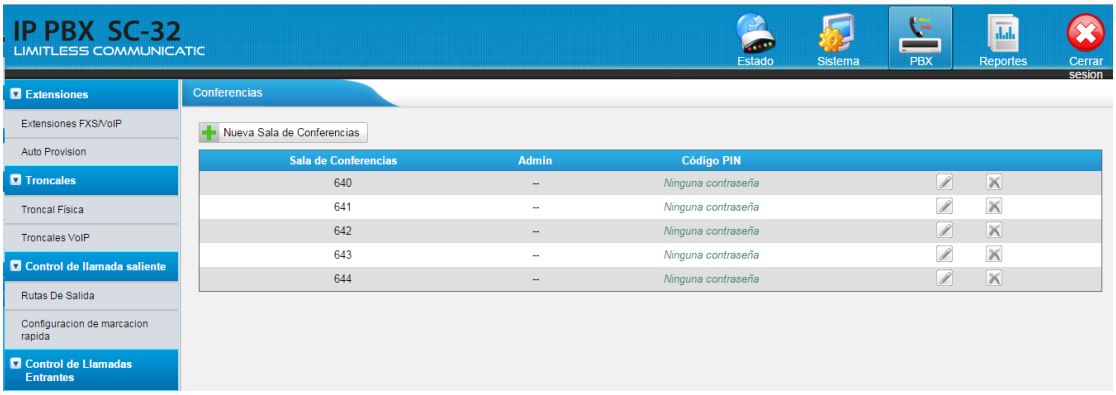


Figura 6-44

Llamadas de Conferencia aumenta la eficiencia y productividad de los empleados, y proporciona una forma más rentable para celebrar reuniones. Agentes de conferencia puede marcar * para acceder a las opciones de configuraciones y el administrador puede quedar el último usuario a afuera y puede bloquear la sala de conferencia.

·Extensión

Este es el número marcado para alcanzar la sala de conferencia.

·Administrador

El administrador puede quedar un usuario a afuera y puede bloquear la sala de conferencia.

·PIN

Estable un PIN que debe ser ingresado para acceder esta sala de conferencia (por ejemplo 1234).

Figura 6-45 Añadir/Editar Sala de Conferencia

6.4.5 Routes Entrante

Enrutamiento entrante procesa el tráfico de llamadas entrantes a las extensiones de destino en horarios oficiales o fuera de horarios oficiales.

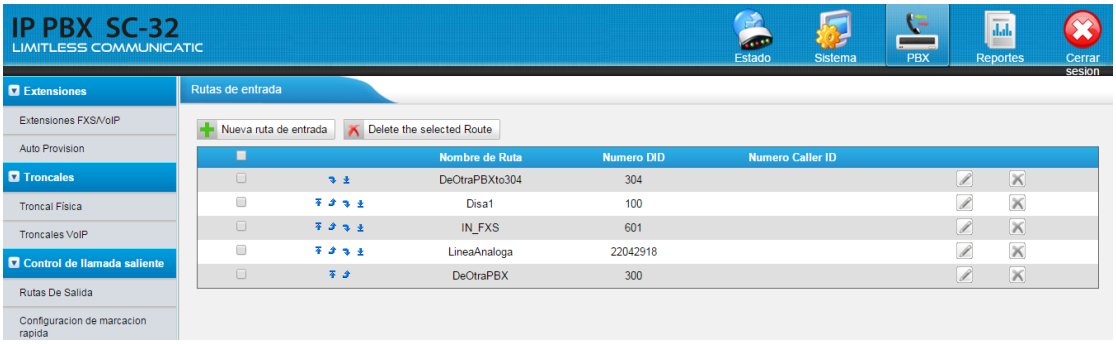


Figura 6-46 Lista de Route Entrante

Hay una route entrante por defecto para todos los troncales y establece IVR como el destino, puede editarlo o crear uno nuevo para sus demandas o puede borrar múltiples routes salientes a la vez si es necesario. Cuando llega una llamada entrante, el sistema comprobará primero "la detección de fax", luego "Vacaciones", por fin "Días Hábiles".

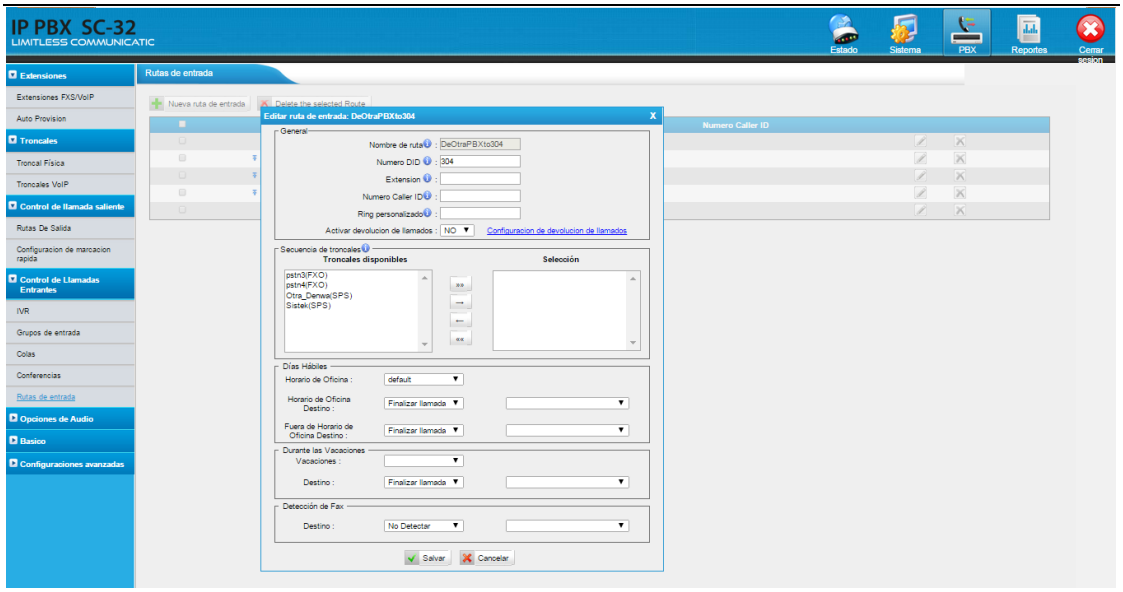


Figura 6-47 Añadir/Editar Route Entrante

1) General

·Nombre de Route

Un nombre para este route entrante. Por ejemplo "pstnin".

·Número DID

Define el número DID esperado si este troncal pase DID en las llamadas entrantes. Deje este campo en blanco para que coincida con las llamadas con unas o sin DID información. También puede utilizar la coincidencia de patrones para que coincida con un rango de números. Los patrones siguientes pueden ser utilizarse:

X: Algún dígito desde 0-9

Z: Algún dígito desde 1-9

N: Algún dígito desde 2-9

[12345-9]: Algún dígito en ménsulas (en este ejemplo, 1, 2, 3, 4, 5, 6, 7, 8, 9)

El "**.**" El carácter coincidirá con todos los dígitos restantes. Por ejemplo, "9011." coincidirá algún número telefónico que empiece con "9011", incluyendo "9011" .

El "**!**" Coincidirá con ninguno dígitos restantes, y hace que el proceso de correspondencia para completar lo antes que se pueda determinar que no hay otros partidos son posibles.

Ejemplo 1: **NXXXXXX** coincidirá algún número telefónico de 7 dígitos.

Ejemplo 2: **1NXXNXXXXX** coincidirá un número telefónico empiece con 1, a continuación por 3 dígitos de área, y luego número de 6 dígitos.

Para más información, por favor consulte a ***Appendix F How to Use DID*.**

·Extensión

Define la extensión para el número DID. Este campo es sólo válido cuando

utilice BRI, SIP, SPS o SPX troncal para éste router entrante. Puede solo ingresar número y "-" en éste campo, y el formato puede ser xxx o xxx-xxx. El recuento del número debe ser único o igual a la cuenta del número DID.

·Número de ID de Llamada

Define el Número de ID de Llamada para ser coincidido en las llamadas entrantes. Deje este campo en blanco para que coincida con unas o sin DID información.

También puede utilizar la coincidencia de patrones (por ejemplo 2[345]X) para que coincida con un rango de números.

Los patrones siguientes pueden ser utilizarse:

X: Algún dígito desde 0-9

Z: Algún dígito desde 1-9

N: Algún dígito desde 2-9

[12345-9]: Algún dígito en ménsulas (en este ejemplo, 1, 2, 3, 4, 5, 6, 7, 8, 9)

El "**.**" El carácter coincidirá con todos los dígitos restantes. Por ejemplo, "9011." coincidirá algún número telefónico que empiece con "9011", incluyendo "9011" .

El "**!**" Coincidirá con ninguno dígitos restantes, y hace que el proceso de correspondencia para completar lo antes que se pueda determinar que no hay otros partidos son posibles.

Ejemplo 1: **NXXXXXX** coincidirá algún número telefónico de 7 dígitos.

Ejemplo 2: **1NXXNXXXXX** coincidirá un número telefónico empiece con 1, a continuación por 3 dígitos de área, y luego número de 6 dígitos.

·Tono Distintivo

UNI-K soporta la asignación a los archivos de tono de llamada personalizados. Por ejemplo, si configura el tono distintivo para tono personalizado a "**Familia**", el tono se reproducirá si el teléfono reciba la llamada entrante.

·Habilita Callback

Puede habilitar la función callback de éste route entrante. Si quiere configurar la función callback, por favor consulte a **chapter 6.7.4**

¿Cómo puedo configurar los tonos distintivos? Por favor consulte a APPENDIX E. Actualmente el tono distintivo puede ser compatible con teléfono Yealink y Snom.

2) Miembros Troncales

Esta área le permite seleccionar que troncales serán miembros de troncales para este route. Para hacer un troncal de ser un miembro de este route, por favor muévelo al cuadro "Seleccionado".

3) Días de Negocios

Define a dónde las llamadas rutarán durante los Días de Negocios.

·Horarios Oficiales

Selecciona un horario oficial de das de negocios definido.

·Destinación en Horarios Oficiales

Configura a dónde se rutan las llamadas entrantes durante los horarios oficiales.

·Termina Llamadas

Ruta las llamadas entrantes a terminar llamadas, el sistema colgará la llamada automáticamente.

·Extensión

Ruta las llamadas entrantes a una extensión especificada.

·Voicemail

Ruta las llamadas entrantes a voicemail de extensión.

·IVR

Ruta las llamadas entrantes a un IVR especificado.

·Grupo de Timbre

Ruta las llamadas entrantes a un Grupo de Timbre especificado.

·Sala de Conferencia

Ruta las llamadas entrantes a una Sala de Conferencia especificada.

·DISA

Ruta las llamadas entrantes a una DISA especificada.

·Cola

Ruta las llamadas entrantes a una Cola especificada.

·Faxes

Ruta las llamadas entrantes a una dirección de mail de extensión especificada.
Nota: Esta función solo soporta T.38 Fax.

·Routes Salientes

Ruta las llamadas entrantes a un route saliente especificado.

Esta función es principalmente utilizada para la conexión de dos sucursales. Por ejemplo: Compañía A es casa matriz que ubicada en USA con una sucursal

B en China. A y B los dos tienen un sistema telefónico UNI-K.
Ahora bien, si el personal de A le quería hacer una llamada a un teléfono o un teléfono móvil en China de la extensión de la A, pero a través de la línea FXS de B, que se puede hacer por esta configuración.

·Destinación en Horarios Fuera de Oficina
Configura a dónde se rutan las llamadas entrantes durante los horarios fuera de oficina.

4) Durante vacaciones
Define a dónde las llamadas rutarán durante vacaciones.

·Vacación
Selecciona qué vacación definida para utilizarse. Cuando un tiempo fue definido en los Días de Negocios y Vacaciones, se lo considerará como vacaciones.

·Destinación
Configura a dónde se rutan las llamadas entrantes durante vacaciones.

5) Detección de Fax
Configura si la detecta faxes en esta route entrante.

Nota: Por favor seleccione IVR como el destino anterior antes de configurar la detección de fax (recomendado).
·Destinación
Configura a dónde las faxes rutarán cuando las faxes fueron detectadas.

·No detecta
No detecta las faxes.

·Email Personalizado
Personaliza una dirección del Email para recibir las faxes. Primero debe configurar el "Configuraciones de Voicemail-> Configuración de SMTP para Voicemail" correctamente antes de utilizar esta opción.

·Faxes
Enviar faxes a una extensión. Si selecciona una extensión FXS aquí, la fax enviará al puerto FXS seleccionado, tiene que conectar una maquina fax a este puerto FXS. Si selecciona una extensión VoIP, la fax enviará al Voicemail de la extensión como un adjuntado.

Nota: Si quiere recibir las faxes con la dirección de Email personalizada, la “Configuraciones SMTP” de “Configuraciones Voicemail” debería ser

configurada con éxito en avanzada. Si quiere recibir las faxes con la dirección de Email configurada en voicemail de la extensión VoIP, debería asegurarse que funciona bien el email probado a su dirección de email.

6.5 Configuraciones de Audio

Avisos personalizados son soportados en UNI-K, y puede cambiar avisos del sistema a avisos de su país local.

6.5.1 Audios Personalizados

Podemos grabar y cargar audios en ésta página; puede también reproducirlo directamente para confirmar si es válido, puede también descargarlo y guardarlo como una copia de seguridad.

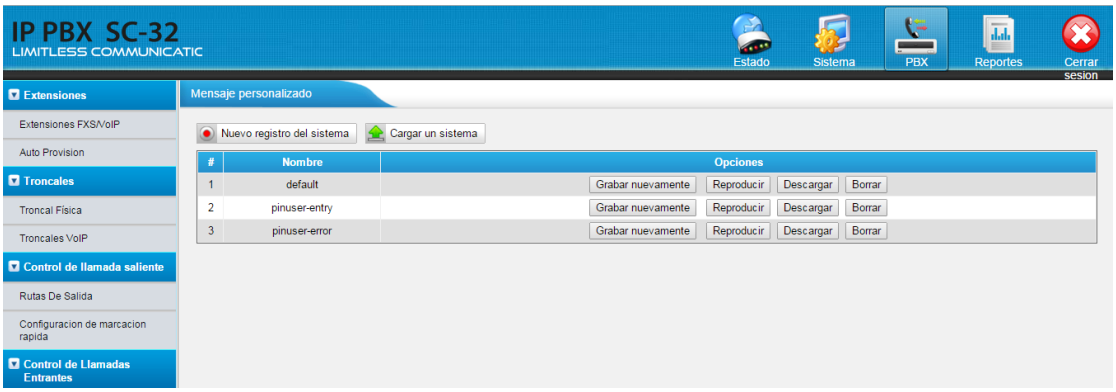


Figura 6-48

1. Grabar un audio nuevo

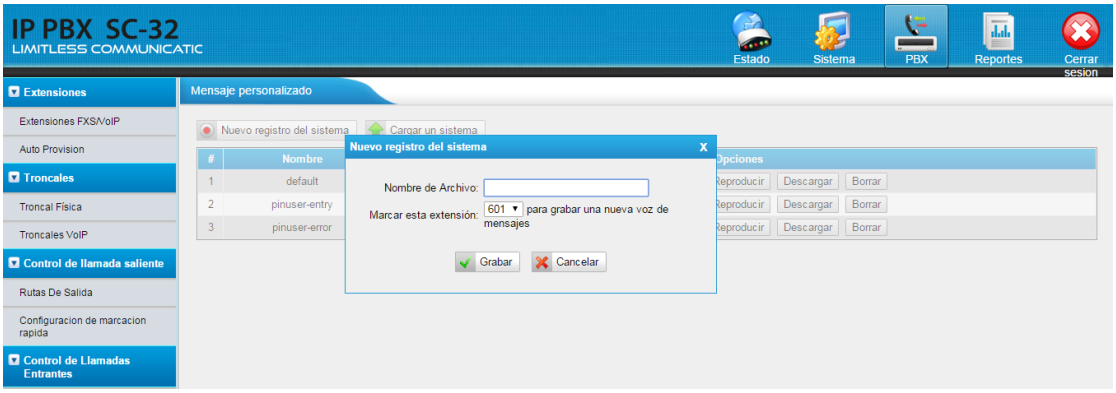


Figura 6-49

El administrador puede grabar audios personalizados mediante los pasos siguientes:
1) Haga clic en "Grabar Audios Personalizados Nuevos".
2) Introduzca el nombre de archivo deseado en la ventana emergente y elija una extensión que llamar para la grabación (por ejemplo, 500).
3) Haga clic en "Grabar". La extensión seleccionada sonará y pueda levantar el teléfono a empezar la grabación.

2. Cargar Audio

Figura 6-50

El administrador puede cargar audios personalizados mediante los pasos siguientes:
1) Haga clic en "Cargar Audio".
2) Haga clic en "Visualizar" para seleccionar el audio deseado.
3) Haga clic en "Cargar" para cargar el audio seleccionado.

Nota: El tamaño del archivo no debe ser mayor que 1.8MB, y el archivo debe ser

del formato WAV:
GSM 6.10 8 kHz, Mono, 1 Kb/s;
Alaw/Ulaw 8 kHz, Mono, 1 Kb/s;
PCM 8 kHz, Mono, 16 Kb/s.

6.5.2 Audios de Música en Espera

En esta página, podemos cargar el audio de música en espera.

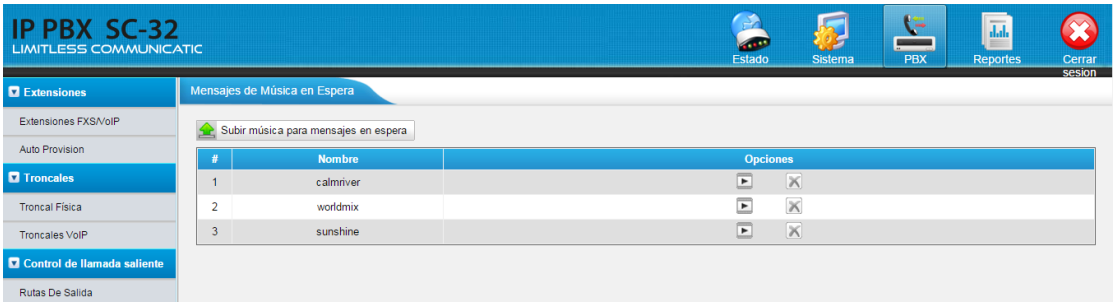


Figura 6-51

El administrador puede cargar la música en espera como los siguientes:
1) Haga clic en "Cargar Audio de Música en Espera".
2) Haga clic en "Visualizar" para seleccionar el audio deseado.
3) Haga clic en "Cargar" para cargar el archivo seleccionado.

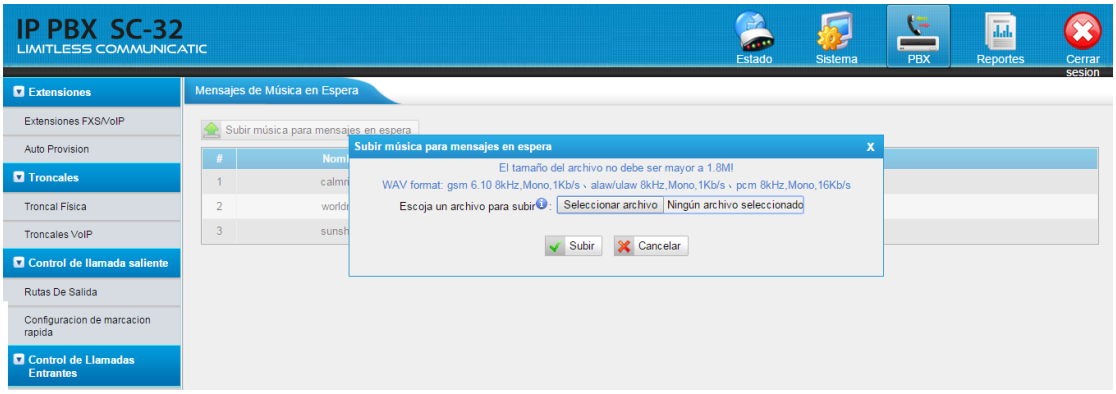


Figura 6-52

Nota: El tamaño del archivo no debe ser mayor que 1.8MB, y el archivo debe ser del formato WAV:
GSM 6.10 8 kHz, Mono, 1 Kb/s;
Alaw/Ulaw 8 kHz, Mono, 1 Kb/s;
PCM 8 kHz, Mono, 16 Kb/s.

6.5.3 Configuraciones de Audios del Sistema

UNI-K tiene audios de varios idiomas. Puede descargar el idioma adecuado que necesita. UNI-K pueden apoyar Inglés Americano, Inglés australiano, chino, holandés, francés, francés canadiense, alemán, griego, húngaro, italiano, polaco, portugués, portugués brasileño, ruso, español, español de México, turco, tailandés y coreano actualmente.

Notas:

1. Es muy recomendable auto detección. Pero si prefiere descargar a través del servidor HTTP o TFTP, por favor póngase en contacto con el distribuidor local para obtener los audios.
2. Cuando se actualiza con éxito, haga clic en "Aplicar cambios" en la web, entonces tendrá efecto, no hay necesidad del reinicio.

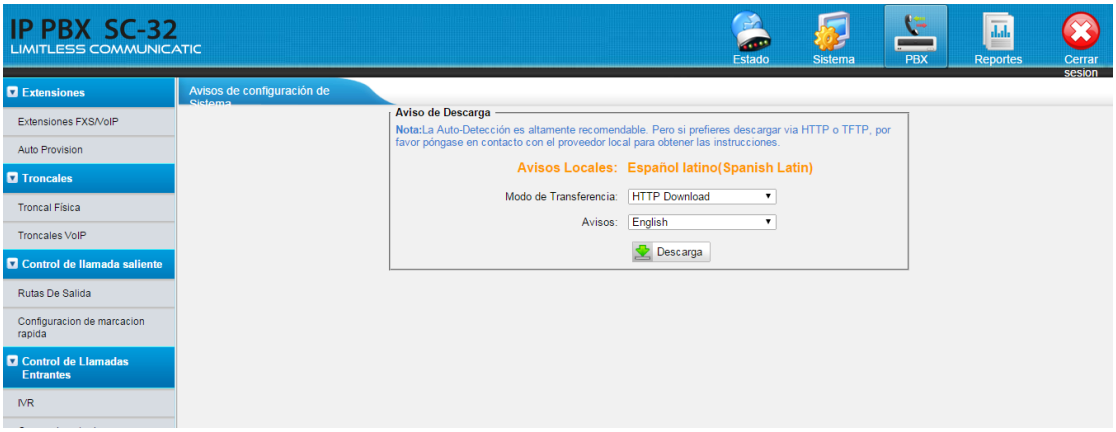


Figura 6-53

6.6 Configuraciones Básicas

Hay unas configuraciones básicas que tenemos que configurar UNI-K UIP PBX SC-32, como Preferencias Generales, Horarios de Negocios, Códigos de Funcionalidades, y Configuraciones de Voicemail.

6.6.1 Preferencias Generales

En esta página, hay unas configuraciones generales de UNI-K.

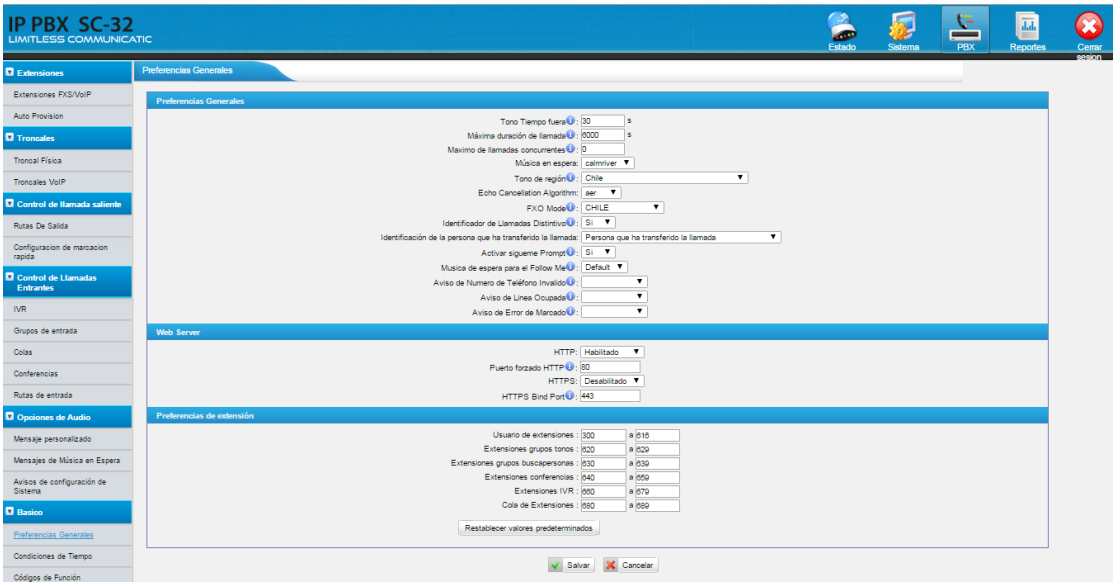


Figura 6-54

1) General

·Timbre de Tiempo Fuera

Número de segundos para que suene un dispositivo antes de manipular la llamada según la configuración Follow Me de la extensión. El valor por defecto es 30s.

.Duración Máxima de Llamadas

La cantidad máxima absoluta de tiempo permitido para una llamada. Una configuración de 0 desactiva Tiempo Fuera. El valor por defecto es 6000s.

.Llamadas Concurrentes Máximas

Límite de las llamadas concurrentes máximas. El valor por defecto 0 significa no hay límite.

· Música en Espera

Se utiliza a establecer música en espera para el sistema.

·Región Tono

Por favor seleccione su país o el país vecino más cerca a habilitar el tono de marcación, tono ocupado, y tono de timbre predeterminado para tu región.

Nota: Por favor reinicie el sistema para tener efecto.

·Puerto unido de HTTP/Puerto de Acceso Web

Puerto que se utiliza para las sesiones HTTP; Por defecto: 80

Nota: Por favor reinicie el sistema para tener efecto.

·FXO Modo
El modo de operación de los puertos FXO.

·Tono Virtual de Timbrado
Es sólo para el troncal GSM/UMTS. Una vez habilitada, cuando el llamador llama afuera con troncales GSM/UMTS, el llamador solamente escuchará el tono virtual timbrado que generado por el sistema antes de la gente contesta la llamada.

·ID de Llamador Distintivo
Cuando las llamadas entrantes se enrutan de grupo de timbre/cola/IVR, las pantallas de identificación de llamada con el nombre del grupo de timbre/cola/IVR, por ejemplo 5503302 (ringgroup_default).

Nota: Para mostrar el nombre de IVR, por favor presione la tecla en lugar del número de extensión directamente.

·Transferencia Atendida de ID de Llamador
Al transferir una llamada utilizando el código de función de transferencia atendida o la tecla de transferencia de teléfono IP, el identificador de llamadores de cesionario o transferidor muestra en la pantalla del destinatario de la llamada. Por defecto la pantalla es el identificador de llamadas del iniciador.
Por ejemplo, si la extensión 500 hace una llamada a extensión 501. Después de 501 atender a llamada, 501 hace una transferencia atendida a la extensión 502. Si selecciona “Transferir”, 502 se mostrará el ID de llamador como 500; si selecciona “Transferir”, 502 se mostrará ID de llamador como 501.

·Audio Follow Me
Cuando se establece "Follow me" a "Transferir a número" en la página de extensión (por ejemplo, cuando 500 es ocupado, transfiere al 501), mientras que 500 está ocupado, la llamada se transferirá al 501. Si “Habilita Audio de Follow Me” seleccionó sí, tendrá audio antes de transferir la llamada. De lo contrario, la llamada será transferida directamente sin algún audio. Por defecto: Sí.

·Música en espera para audio de Follow Me
Configura si reproduce un audio “por favor aguarde en cuando estoy tratando a ubicar la persona que llame” cuando transfiere una llamada por la configuración de follow me.

·Audio del Número Telefónico Inválido
Configura el audio cuando el número telefónico marcado es inválido.

·Audio de Línea Ocupada
Configura el audio cuando el número telefónico marcado es ocupado.

·Audio de Marcado Fallado
Configura el audio cuando el marcado fallado causado por conexión o un canal no válido.

2) Servidor Web
·HTTP
Activa o desactiva la sección HTTP.

·Puerto HTTP Unido
El puerto predeterminado a utilizarse para la sección HTTP es 80.

·HTTPS
Activa o desactiva la sección HTTPS.

·Puerto HTTPS Unido
El puerto predeterminado a utilizarse para la sección HTTPS es 443.

Nota: Por favor reinicie el sistema para tener efecto.

3) Preferencias de Extensión
·Extensiones del Usuario
El valor predeterminado es 500 a 616.

·Extensiones del Grupo de Timbre
El valor predeterminado es 620 a 629.

·Extensiones del Grupo Paging
El valor predeterminado es 630 a 639.

·Conferencia de Extensiones
El valor predeterminado es 640 a 659.

·IVR de Extensiones
El valor predeterminado es 660 a 679.

·Cola de Extensiones
El valor predeterminado es 680 a 689.

6.6.2 Horarios de Negocios

configuración de horarios de negocios incluyendo "Vacaciones" que es utilizada para controlar las llamadas entrantes, podemos configurar en esta página.

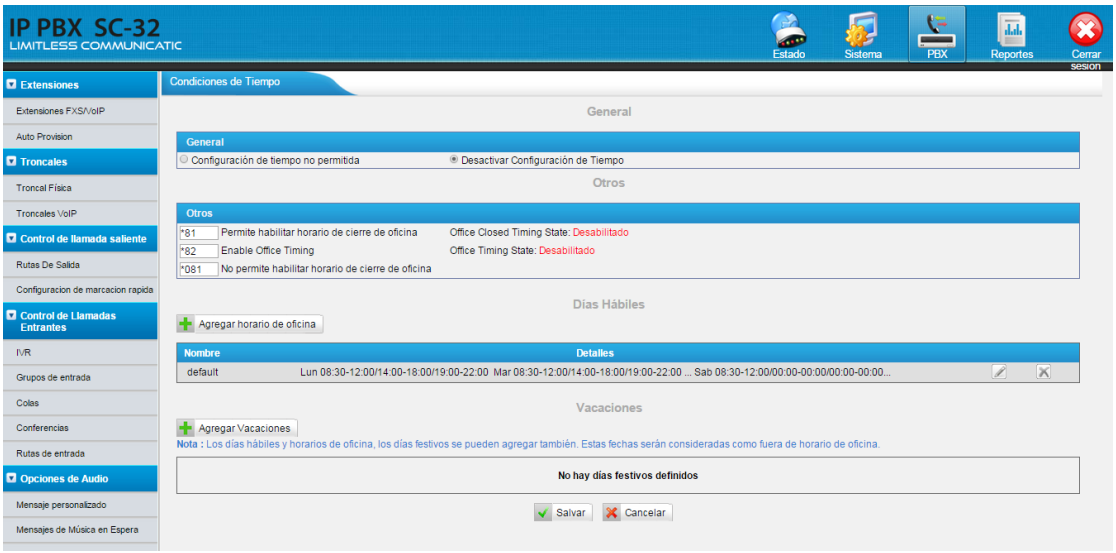


Figura 6-55

1) General

·Activa Horarios de Negocios

·Desactiva Horarios de Negocios

2) Otras

·Activa Horarios Cerrados de Oficina

Mediante el marcado *81 (*81 es el código predeterminado) en una extensión forzará el tiempo cerrado de oficina para el depósito no importa cómo es la configuración general.

·Activa Horarios de Oficina

Mediante el marcado *82 (*82 es el código predeterminado) en una extensión forzará el tiempo de oficina para el depósito no importa cómo es la configuración general.

·Desactiva Horarios Cerrados de Oficina

Mediante el marcado *081 (*081 es el código predeterminado) en una extensión desactivará Horarios Cerrados de Oficina.

3) Agregar horarios oficiales.

Puede establecer horarios de negocios aquí.

4) Agregar Vacación.

Puede establecer vacación aquí.

Si un período de tiempo es configurado como vacaciones y horarios oficiales

también, se considerará como vacaciones.

6.6.3 Códigos de Funciones

Hay muchos códigos de funciones disponibles en UNI-K, que permiten los usuarios a marcar desde la parte extensión a realizar la función exacta.

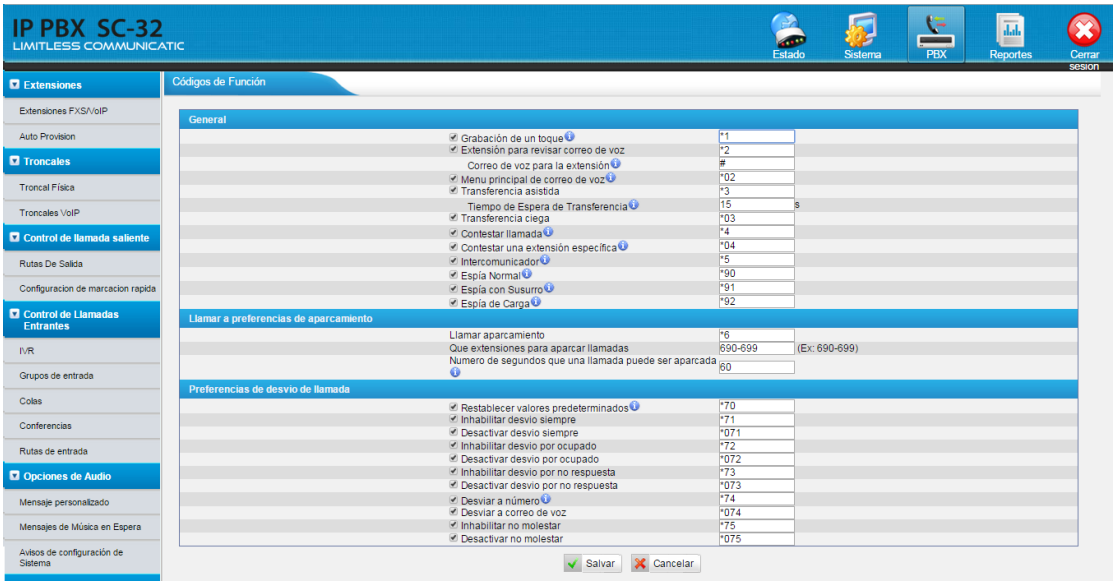


Figura 6-56

1) General

·Grabación con Un Taque

Un usuario puede iniciar o determinar la grabación de llamada mediante el marcado *1 durante una llamada. (*1 es configuración predeterminada).

·Extensión para Revisar Voicemail

Los usuarios puede revisar sus Voicemail mediante el marcado *2 en sus teléfonos (*2 es la configuración predeterminada).

·Voicemail para Extensión

Los usuarios pueden dejar un voicemail a otras extensiones mediante el marcado # en sus teléfonos o llamada entrante puede ser reenviada al voicemail de una extensión directamente. (# es configuración predeterminada).

Por el ejemplo, la extensión 500 quiere dejar un mensaje para la extensión 501, los usuarios pueden utilizar 500 marcando "#501" a entrar el voicemail de 501.

·Menú Principal de Voicemail

Los usuarios pueden visitar el menú principal mediante el marcado *02 (*02 es la configuración predeterminada).

·Transferencia Atendida
Los usuarios puede transferir una llamada entrante mediante el marcado *3 en sus teléfonos (*3 es la configuración predeterminada).

·Transferencia Atendida en Tiempo fuera
El valor de tiempo fuera de transferencia una llamada.

·Transferencia Ciega
Los usuarios puede transferir en ciega una llamada entrante mediante el marcado *03 en sus teléfonos (*03 es la configuración predeterminada).

·Llamada Pickup
Los usuarios puede detener una llamada entrante mediante el marcado *4 en sus teléfonos (*4 es la configuración predeterminada).

·Extensión Pickup
Los usuarios puede detener la llamada entrante de una extensión específica mediante el marcado *04+extensión en sus teléfonos (*04 es la configuración predeterminada).

·Intercom
Define el código de función que se utiliza a marcar una extensión en el modo intercom. Por ejemplo, establecer este valor a *5 se permitirá iniciar una llamada de intercomunicación con la extensión 501 marcando *5501.

·Monitoreo Normal
En este modo, puede solamente escuchar la extensión monitoreada, por ejemplo puede marcar *90501 a monitorear la extensión 501.

·Monitoreo Susurro
En este modo, puede escuchar/susurrar a la extensión monitoreada, por ejemplo, puede marcar *90501 a escuchar la extensión 501, y también puede hablar con 501.

·Monitoreo Completo
En este modo, puede irrumpir en ambas extensiones que participan en la llamada, por ejemplo, puede marcar *92501 a escuchar y hablar con las extensiones de ambas partes.

2) Preferencias de Parar Llamada
·Aparcamiento de Llamadas
El usuario puede aparcar una llamada entrante en su teléfono propio mediante

presionar "*6" (*6 es la configuración predeterminada)

·Rango de Extensión utilizado para aparcar llamadas
El usuario puede aparcar una llamada entrante en una extensión diseñada primero y luego atender la llamada nuevamente en la otra extensión.

·Número de segundos que una llamada puede ser aparcada antes de ser re llamada.
Define el tiempo (en segundos) que una llamada puede aparcada antes de ser re llamada a la estación que aparcada.

3) Preferencias de Desvío Llamadas
·Restablecer al Predeterminado
Los usuarios puede restablecer todos predeterminados de desvío de llamadas mediante el marcado *70 en sus teléfonos (*70 es la configuración predeterminada).

Nota: ·Cuando restablecer al Predeterminado. Las configuraciones del desvío de llamadas se configurarán como los siguientes:
Desvío siempre: Desactivado
Desvío de ocupado a Voicemail: Activado
Sin contesta desvío a Voicemail: Activado
No molesta: Desactivado

·Activa Desvío Todas Llamadas
Los usuarios pueden activar desvío siempre mediante el marcado *71 en sus teléfonos (*71 es la configuración predeterminada).

·Desactiva Desvío Todas Llamadas
Los usuarios pueden desactivar desvío siempre mediante el marcado *071 en sus teléfonos (*071 es la configuración predeterminada).

·Activa Desvío Cuando Está Ocupado
Los usuarios pueden activar ocupado desvío mediante el marcado *72 en sus teléfonos (*72 es la configuración predeterminada).

·Desactiva Desvío Cuando Está Ocupado
Los usuarios pueden desactivar ocupado desvío mediante el marcado *072 en sus teléfonos (*072 es la configuración predeterminada).

·Activa Desvío Sin Contesta
Los usuarios pueden activar desvío sin contesta mediante el marcado *73 en sus teléfonos (*73 es la configuración predeterminada).

·Desactiva Desvío Sin Contesta
Los usuarios pueden desactivar desvío sin contesta mediante el marcado *073 en sus teléfonos (*073 es la configuración predeterminada).

·Desvía a número
Los usuarios pueden activar desvío de llamadas mediante marcado este código de función, siguiendo número de la extensión o teléfono a desviar todas las llamadas a este número.

Nota: Los usuarios pueden activar desvío a número mediante el marcado *74 + número telefónico. Por ejemplo mediante el marcado *74501, todas las llamadas desviarán a la extensión 501.

·Desvía a Voicemail
Los usuarios puede desviar la llamada a Voicemail mediante el marcado *074 en sus teléfonos (*074 es la configuración predeterminada).

·Activa No Molesta
Los usuarios pueden activar No Molesta mediante el marcado *75 en sus teléfonos (*75 es la configuración predeterminada).

·Desactiva No Molesta
Los usuarios pueden desactivar No Molesta mediante el marcado *075 en sus teléfonos (*075 es la configuración predeterminada).

6.6.4 Configuraciones de Voicemail

En esta página, podemos configurar unas configuraciones para la funcionalidad de voicemail, incluyendo configuraciones generales de voicemail y SMTP, cual es utilizado para "voicemail a email".

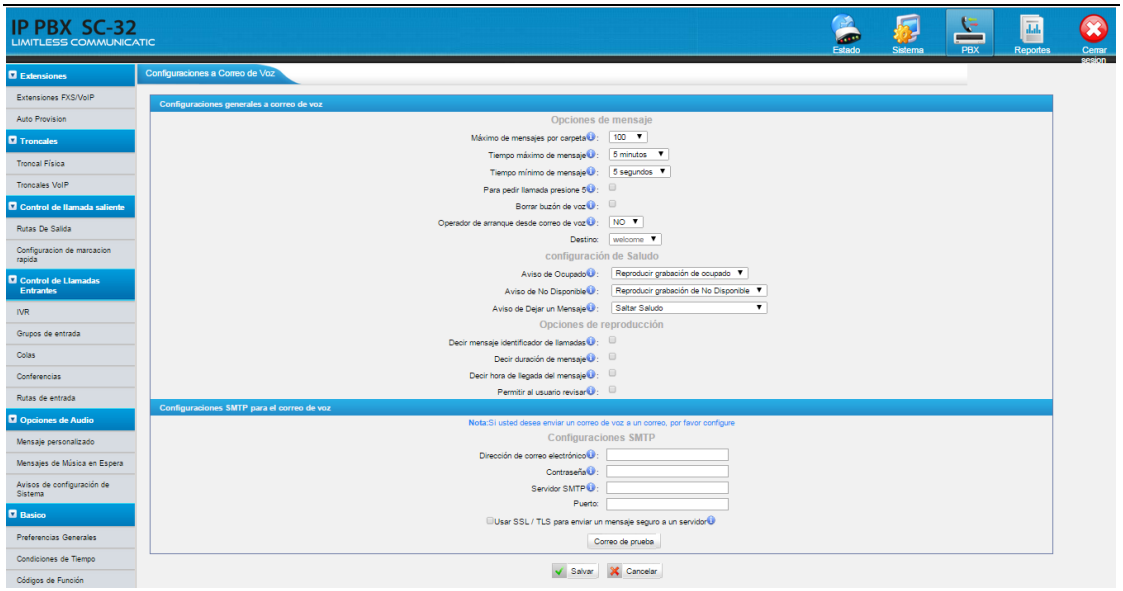


Figura 6-57

1) Configuraciones Generales de Voicemail

a) Opciones de Mensaje

·Mensajes Máximos por Carpeta

Establece el número máximo de mensajes que puede ser guardado en un buzón sola de voicemail.

·Tiempo Máximo de Mensaje

Establece longitud máxima de un mensaje solo de voicemail.

·Tiempo Mínimo de Mensaje

Establece longitud mínima de un mensaje solo de voicemail. Mensajes por debajo de este umbral se eliminarán de forma automática.

·Pide al Llamador a marcar 5

Si esta opción es establecida, el llamador será avisado a marcar 5 antes de dejar un mensaje.

·Operador Salirse desde Voicemail

Si esta opción es establecida, el llamador puede salir del voicemail y entra al destino (IVR) mediante el marcado "0".

b) Configuraciones de Bienvenida

·Anuncio de Ocupado

Reproduce Bienvenida cuando la extensión llamada es ocupada.
Omitir Bienvenida: No reproduce la bienvenida.
Reproduce bienvenida de ocupado: Reproduce bienvenida de la extensión

ocupada.

·Anuncio Disponible
Reproduce Bienvenida cuando la extensión llamada es disponible
Omitir Bienvenida: No reproduce la bienvenida.
Reproduce bienvenida disponible: Reproduce bienvenida de la extensión disponible.

·Anuncio de Deje un Mensaje
Reproduce bienvenida a pedir el llamador a marcar 5 para dejar un mensaje.
Omitir Bienvenida: No reproduce la bienvenida.
Reproduce bienvenida de ocupado: Reproduce bienvenida de la extensión ocupada.
Reproduce bienvenida disponible: Reproduce bienvenida de la extensión disponible.

c) Opciones de Reproducción
·Anuncia ID de Llamador de Mensaje
Si esta opción es activada, La ID del llamador de la parte que deja el mensaje reproducirá antes de empezar la producción del mensaje de Voicemail.

·Anuncia la Duración del Mensaje
Si esta opción es activada, La duración del mensaje en minutos reproducirá antes de empezar la producción del mensaje de Voicemail.

.Anuncia el Tiempo Llegado del Mensaje
Si esta opción es activada, el tiempo llegado del mensaje reproducirá antes de empezar la producción del mensaje de Voicemail.

.Permitan los Usuarios a visualizar los Mensajes
Permitan los llamadores a visualizar sus mensajes grabados antes de enviarlo a voicemail.

2) Configuraciones de SMTP para Voicemail
Nota: Si quiere enviar voicemail mensajes como email adjuntado, por favor configura esta sección.

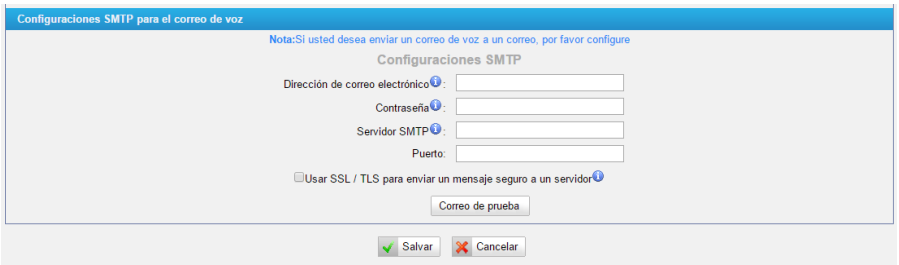

Configuraciones SMTP para el correo de voz
Nota:Si usted desea enviar un correo de voz a un correo, por favor configure
Configuraciones SMTP
Dirección de correo electrónico:
Contraseña:
Servidor SMTP:
Puerto:
Usar SSL / TLS para enviar un mensaje seguro a un servidor
Correo de prueba
Salvar
Cancelar

Figura 6-58

·Dirección de E-mail
la dirección del E-mail que UNI-K utilizará a enviar voicemail.

·Contraseña
La contraseña para la dirección de E-mail utilizada anteriormente.

·SMTP Servidor
La dirección IP o hostname de un SMTP servidor que UNI-K se conectará para que envíe los mensajes de voicemail por vía email, por ejemplo mail.yourcompany.com.

·Puerto
SMTP Puerto: el valor predeterminado es 25.

·Utiliza SSL/TLS a enviar mensajes de seguridad al servidor
Si el servidor de envío el email requiere a autenticar el envidador, tiene que seleccionar el buzón para revisar.
Nota: Debería ser seleccionado para Gmail o servidor de intercambio.
Después de completar las informaciones anteriores, puede hacer clic en botón "Probar Configuraciones de Cuenta" a revisar si la configuración está OK o no.
1) Si la prueba es exitosa, puede utilizar el email seguramente.
2) Si la prueba falla, compruebe si la información anterior es correcta o si la red está bien.

6.7 Configuraciones Avanzada

6.7.1 Configuraciones de SIP

1) General

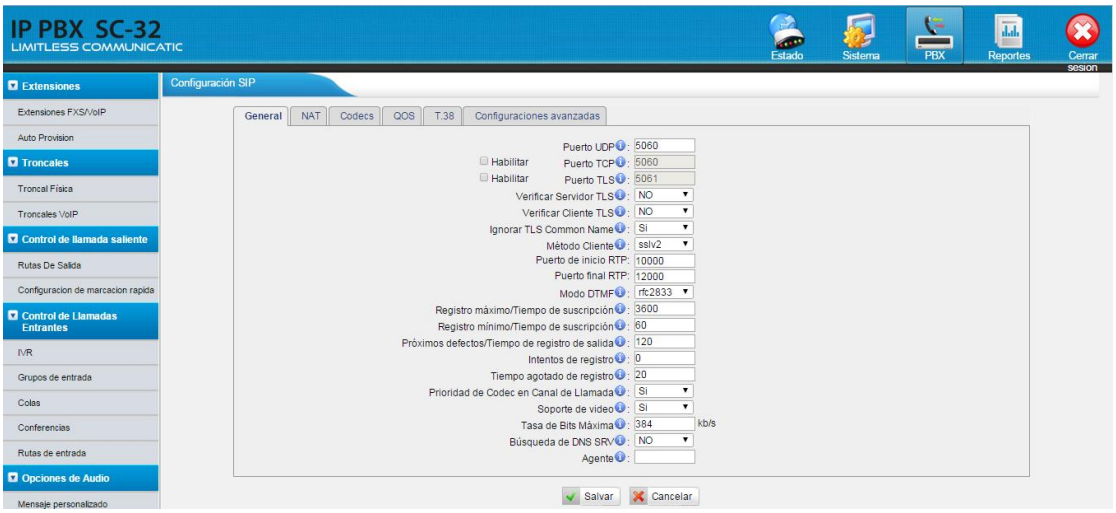


Figura 6-59

·UDP Puerto
Puerto utilizado para los registros SIP. Es 5060 segundos por defecto.

·TCP Puerto
Puerto utilizado para los registros SIP. Es 5060 segundos por defecto.

·TLS Puerto
Puerto utilizado para los registros SIP. Es 5061 segundos por defecto.

·TLS Servidor de Compruebe
Cuando utilizando UNI-K como un cliente TSL, sí o no para verificar el certificado del servidor. Es "No" por defecto.

·TLS Cliente de Compruebe
Cuando utilizando UNI-K como un servidor TSL, sí o no para verificar el certificado del servidor. Es "No" por defecto.

·TLS Ignore Nombre Común
Establece este parámetro como "No", y el nombre común debe ser el mismo con IP o el nombre de domain.

·TLS Cliente Método
Cuando utilizando UNI-K como TLS cliente, especifique el protocolo para la conexión TLS saliente. Puede seleccionarlo como tlsv1, sslv2 o sslv3.

·Inicio de RTP Puerto
Inicio del rango de RTP puerto.

·Terminación de RTP Puerto
Terminación del rango de RTP puerto.

·DTMF modo
Establece modo predeterminado para enviar DTMF. Configuración predeterminada: rfc2833

·Registro Máximo/Veces de Suscripción
Duración máxima (en segundos) de un registro SIP. El valor predeterminado es 3600 segundos.

·Registro Mínimo/Veces de Suscripción
Duración mínimo (en segundos) de un registro SIP. El valor predeterminado es 60 segundos.

Las veces Predeterminadas de Registro Entrante/Saliente

Las veces Predeterminadas de Registro Entrante/Saliente: Duración predeterminada (en segundos) del registro Entrante/Saliente.

·Intento de Registro

El número de mensajes de SIP REGISTRO para enviarse a un SIP Registrador antes de abandonarse. El valor por defecto es 0 (no hay límite).

·Tiempo Afuera de Registro

Número de segundos a esperar para una respuesta viene de un SIP Registrador antes de considerarse que el registro está en tiempo afuera. El valor predeterminado es 20 segundos.

·Prioritario de Código de Canal de Llamada

Una vez activada, cuando marque hacia afuera vía troncales SIP/SPS, el código de canal de llamada será seleccionado en la preferencia. Si no, UNI-K seguirá el prioritario en sus troncales SIP/SPS.

·Vídeo Soporta

Soporta para SIP vídeo o no. Por defecto es sí.

·Bit Rimo Máximo

Configura bit máximo para la pantalla de vídeo. Por defecto: 384kb/s

·DNS SRV Búsqueda

Por favor activa esta opción cuando su troncal SIP contiene más que una dirección IP.

·Usuario Agente

Para cambiar el parámetro de usuario agente de Asterisk, el predeterminado es "UNI-K"; puede cambiarlo si es necesario.

2) NAT

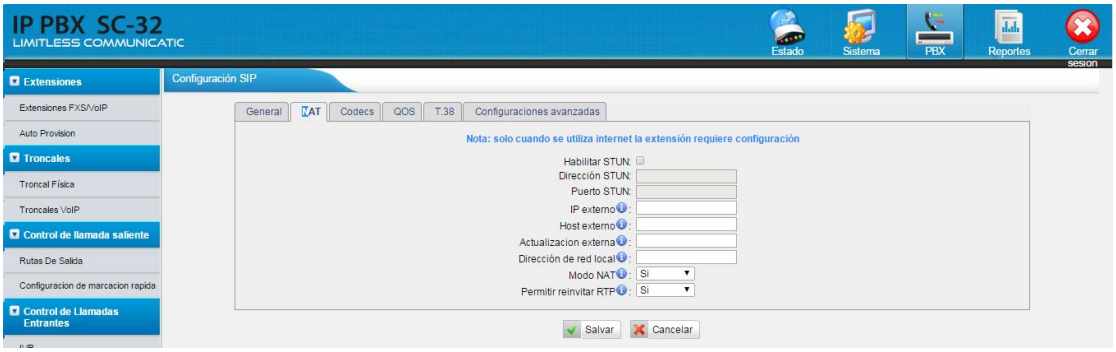


Figura 6-60

Nota: Configuración de esta sección es solo requerido cuando utiliza extensión remota.

·Activa STUN
STUN (Simple Trasversal of UDP through NATs) es un protocolo para ayudar a los dispositivos detrás de un firewall NAT o router con su enrutamiento de paquetes.

·STUN Dirección
El servidor STUN permite a los clientes a encontrar su dirección pública, el tipo de NAT están detrás y el puerto lateral de internet asociados por el NAT con un puerto local particular. Esta información se utiliza para establecer UDP comunicación entre el cliente y el proveedor de VOIP y así establecer una llamada.

·Dirección IP Externa
la dirección IP que será asociada con mensajes SIP saliente si el sistema es en un NAT medio ambiente.

·Host Externo
Alternativamente se puede especificar un host externo, y el sistema realizará las consultas DNS periódicamente.
Esta configuración sólo es necesaria cuando tu dirección IP pública no es estática. Se recomienda que se utilice una dirección IP estática pública con este sistema. Para más información por favor póngase en contacto con su ISP.

·Intervalo de actualización externos
Si se ha proporcionado un host externo, se puede especificar cómo a menudo el sistema realizará una consulta DNS en este host. Este valor es especificado en segundos.

·Identificación de Red Local
Utilizado para identificar la red local mediante un par de máscara de número/suben de red cuando el sistema está detrás de un NAT o firewall.
Unos ejemplos de este son los siguientes:
"192.168.0.0/255.255.0.0": Todas las direcciones de RFC 1918 son de redes locales;
"10.0.0.0/255.0.0.0": También RFC1918;

"172.16.0.0/12":Otro RFC1918 con CIDR notación;
"169.254.0.0/255.255.0.0": Cero red local conf.
Para más información por favor consulte a RFC1918.

·NAT Modo

Configuración de NAT global para el sistema; las opciones para esta configuración son como los siguientes:
sí = Use NAT. Ignora la información de dirección en las cabeceras SIP/SDP y responde a la dirección/puerto IP del remitente.
No = Use NAT modo sólo corresponde a RFC3581.
Nunca= Nunca trate de modo NAT o RFC3581 soporte.
Route = use NAT pero no incluyen puerto en las cabeceras.

·Permite RTP Re invite

De forma predeterminada, el sistema enrutara los vástagos de los medios de comunicación desde los extremos de la SIP a través de sí mismo. Activa esta opción hace que el sistema intenta a negociar los puntos finales para enrutara paquetes entre ellos directamente, saltándose el sistema. No es siempre posible que el sistema negociar los medios de comunicación de extremo a extremo por enrutamiento.

3) Códigos

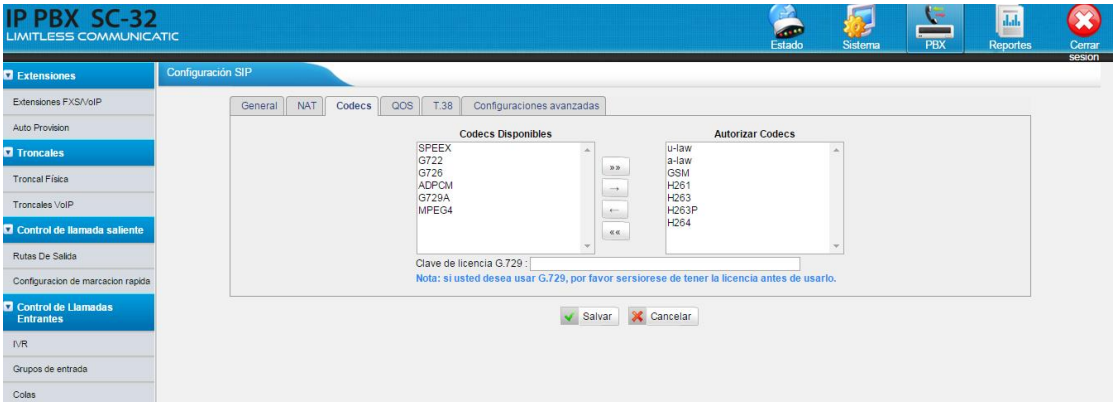


Figura 6-61

Un código es un algoritmo de compresión o descompresión que usa en la transmisión de los paquetes de voz sobre una red o Internet.
ala: Un código estándar de PSTN, utilizado en Norteamérica, que proporciona una calidad muy buena voz y consume 64kbit/s en cada dirección (recepción y transmisión) de una llamada VoIP.

a-la: Un código estándar de PSTN, utilizado afuera de Norteamérica, que proporciona una calidad muy buena voz y consume 64kbit/s en cada dirección (recepción y transmisión) de una llamada VoIP.

GSM: Un código estándar inalámbrico,, utilizado en el mundo, que proporciona una calidad de voz adecuada y consume 13.3kbit/s en cada dirección (recepción y transmisión) de un llamada VoIP. GSM es soportado por muchos teléfonos VoIP.

SPEEX: Ápex es un Open So urce/Free Software formato de compresión de audio libres de patentes diseñado para discurso. El proyecto Speex pretende bajar la barrera de entrada para aplicaciones de voz al proporcionar una alternativa libre a propietarios caro discurso códigos. Además, Speex está bien adaptado a las aplicaciones de Internet y ofrece características útiles que no están presentes en la mayoría de otros códigos.

G.722:G.722 es una voz en banda ancha algoritmos de codificación compatible con la velocidad de bits de 48, 56 y 64 kbps de banda ancha. Es una banda ancha de codificación de voz de la serie G.

G.726: Un código de PSTN, utilizado en el mundo, que proporciona una calidad de voz adecuada y consume 32kbit/s en cada dirección (recepción y transmisión) de un llamada VoIP. G.726 es soportado por muchos teléfonos VoIP.

ADPCM, G.729A, H261, H263, H263p, H264, MPEG4.
Nota: Si quería utilizar G.729, por favor ingrese su licencia.

4) QoS

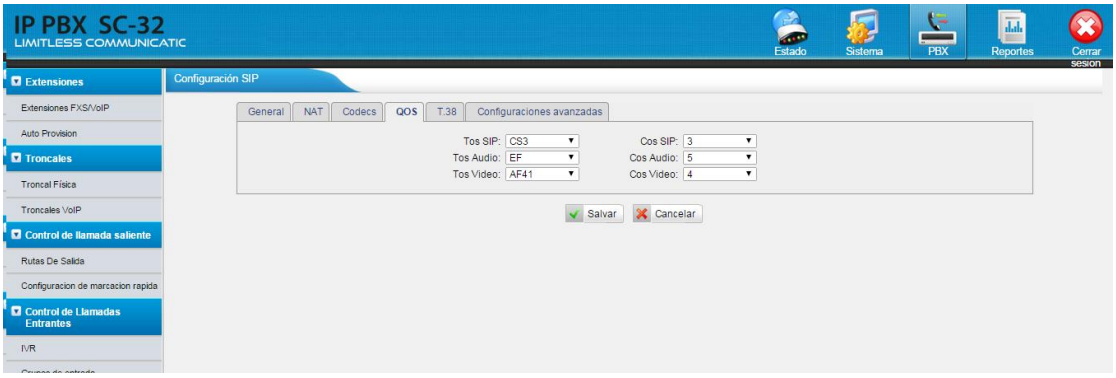


Figura 6-62

QoS (Quality of Service) es un tema importante en las implementaciones de VoIP. La cuestión es cómo garantiza ese tráfico de paquetes de voz o la conexión de otros medios de comunicación no será retrasada o cayó debido interferencia de otro tráfico de prioridad baja. Cuando la capacidad de la red es insuficiente, QoS podría dar prioridad a los usuarios por el valor configurado.

5) T.38

Figura 6-63

·Re-invite SDP No Agrega Atributos T.38

Si establece en sí, SDP en re-invite a paquete no agregarán T.38 atributos.

·Corrección Error

Re-invite SDP T38FaxUdpEc.

·T38 Max BitRate

Configura T38 Max Bitrate.

6) Configuraciones Avanzada

Figura 6-64

·Desde Campo

Donde consigue el ID en el paquete SIP.

·A Campo

Donde consigue el DID en el paquete SIP.

·180 Sonido

Se establece cuando el proveedor de telecom necesite. Normalmente no es necesario.

·Partido ID Remoto
Si desea enviar remoto-partido-ID de cabecera de SIP o no. Por defecto: no.

·Permite Guest
Si se permite registro anónimo de la extensión o no. Por defecto: no.
Esta opción se utiliza para evitar algunas llamadas anónimas por hackers. Para más detalles sobre la configuración de la seguridad del sistema, por favor consulta **APPENDIX B UNI-K Security Configuration Guide**

·Pedantic
Activa el pedantic parámetro. Por defecto: no.

·Alwaysauthreject
Si se activa, cuando UNI-K rechaza paquetes "Register" o "Invite", UNI-K responden siempre los paquetes usando "SIP404 no encontrado".

·OPTIONS Response 200
Si establece en sí, la respuesta a una OPCIONES es siempre 200 OK.

·Sesión-temporizadores
Activa el modo de Sesión-temporizadores, por defecto: Sí

·Sesión-expira
El intervalo de actualización máx.

·Sesión-minSe
El intervalo de actualización mínimo, que no debe ser inferior a 90s.

·Sesión-actualización
Selecciona sesión-actualización, por defecto es Uas.

6.7.2 Configuraciones de IAX

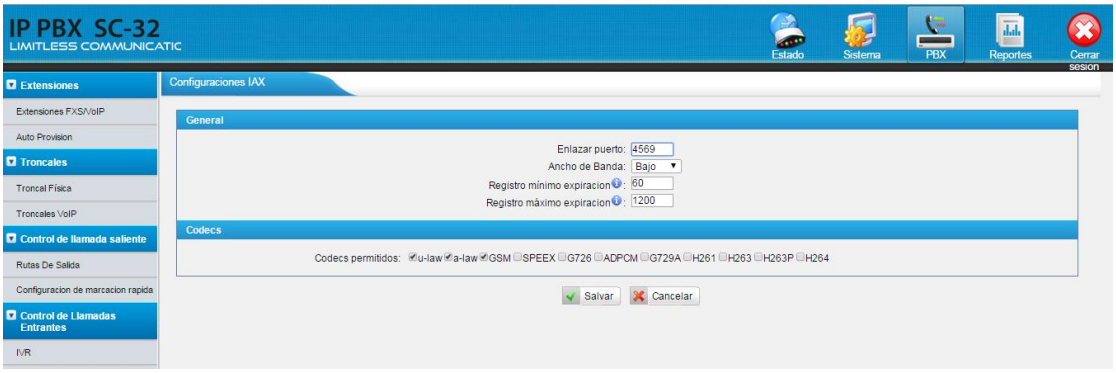


Figura 6-65

1) General

·Puerto Unido
Puerto utilizado para los registros IAX2. Es 4569 por defecto.

·Banda Ancha
Baja/media/alta con esta opción usted puede controlar qué código a utilizar.

·Tiempo de Registro Mínimo
Duración mínimo (en segundos) de un registro IAX2. El valor predeterminado es 60 segundos.

·Tiempo de Registro Máximo
Duración máxima (en segundos) de un registro IAX2. El valor predeterminado es 1200 segundos.

2) Códigos
Un código es un algoritmo de compresión o descompresión que usa en la transmisión de los paquetes de voz sobre una red o Internet.
u-law: Un código estándar de PSTN, utilizado en Norteamérica, que proporciona una calidad muy buena voz y consume 64kbit/s en cada dirección (recepción y transmisión) de una llamada VoIP.

a-law: Un código estándar de PSTN, utilizado afuera de Norteamérica, que proporciona una calidad muy buena voz y consume 64kbit/s en cada dirección (recepción y transmisión) de una llamada VoIP.

GSM: Un código estándar inalámbrico,, utilizado en el mundo, que proporciona una calidad de voz adecuada y consume 13.3kbit/s en cada dirección (recepción y transmisión) de un llamada VoIP. GSM es soportado por muchos teléfonos VoIP.

SPEEX: Speex es un Open Source/Free Software formato de compresión de audio libres de patentes diseñado para discurso. El proyecto Speex pretende bajar la barrera de entrada para aplicaciones de voz al proporcionar una alternativa libre a propietarios caro discurso códigos. Además, Speex está bien adaptado a las aplicaciones de Internet y ofrece características útiles que no están presentes en la mayoría de otros códigos.

G.726: Un código de PSTN, utilizado en el mundo, que proporciona una calidad de voz adecuada y consume 32kbit/s en cada dirección (recepción y transmisión) de un llamada VoIP. G.726 es soportado por muchos teléfonos VoIP.

ADPCM, G.729A, H261, H263, H263p, H264.
Nota: Si quería utilizar G.729, por favor ingrese su licencia.

6.7.3 Lista Negra

La lista negra es utilizada a bloquear una llamada entrante/saliente. Si el número de llamada entrante/saliente es registrado en el número de la lista negra, el llamador escuchará el audio siguiente: "El número marcado no está en servicio. Por favor, compruebe el número e inténtelo de nuevo". El sistema desconectará luego la llamada.

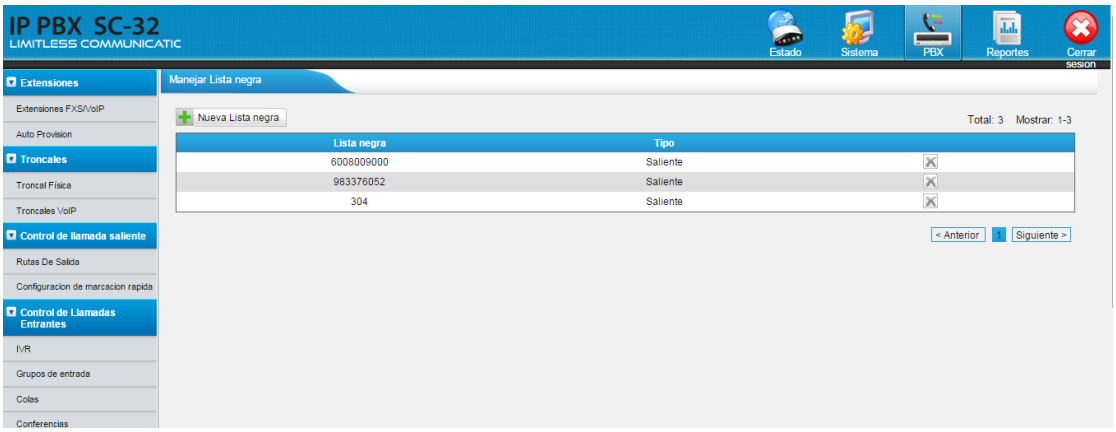


Figura 6-66

Podemos agregar un número con el tipo: entrante, saliente o ambos.

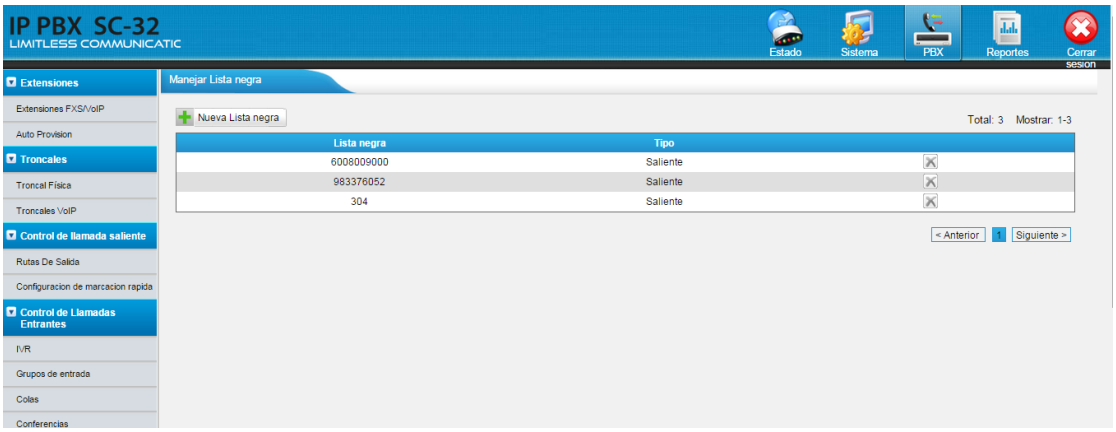


Figura 6-67

Nota: Añadir un número telefónico en la lista negra, tal como "05921234567":

1) Si el tipo es "entrante", luego este número no puede ser llamado.
2) Si el tipo es "saliente", luego las extensiones en UNI-K no puede llamar este número.

6.7.4 Configuraciones de Callback

UNI-K permite llamador A marcar un número de ruta entrantes, y después de escuchar el timbre, A puede colgar la llamada o esperar UNI-K cortar la llamada, luego UNI-K llamará al A con este número. Cuando A atiende la llamada, A puede marcar el número que quiere a llamar; UNI-K se comunique el número con su ruta saliente.

Notas:

1. Si desea utilizar la función de callback, por favor asegúrese de que está habilitado en el panel de configuración de ruta entrante.
2. No hay reglas de callback necesitan para ser establecidas si el troncal soporta callback con el ID de llamador directamente.

Figura 6-68

·Permitan Todos Números

Si quiere aplicar la función de Callback a todos los números entrantes, por favor a validar Permiten Todos Números.

Sigue los pasos debajo a utilizar esta función.

Paso 1: Habilita Callback.

Rutas Entrantes - Selecciona “sí” en “Habilita Callback” a habilitar esta función.

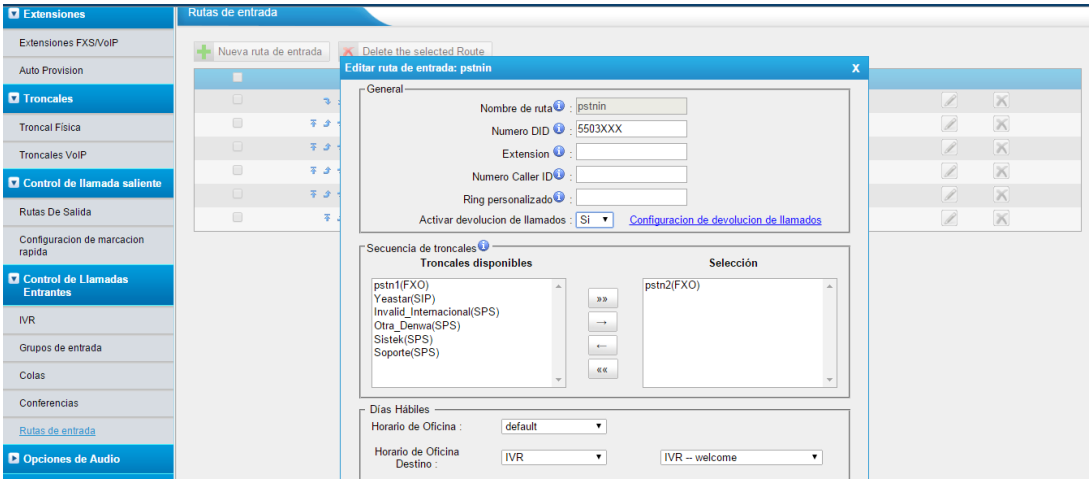


Figura 6-69

Paso 2: Crea Número Callback

Figura 6-70

Paso 3: Crea Reglas de Callback

Necesitaría a crear reglas de Callback cuando el sistema debe despojar o añadir dígitos.

Figura 6-71

·Nombre de Troncal

Selecciona el troncal con reglas de Callback.

·Dígitos Cifrados del frente

Define cuantos dígitos cifrarán desde la llamada en número antes de realizarse Callback. Por ejemplo, cuando llama desde el número 123456789 a UNI-K, el ID de llamador es 0123456789, pero solo puede llamar 123456789 exitosamente desde el troncal de UNI-K. Debería configurar el número 0123456789 como el número de callback y cifra 1 dígito antes de realizarse el Callback.

·Anteponer antes del Marcado

Define dígitos agregados antes de un número de Callback antes de de realizarse callback. Por ejemplo, el número de llamada (ID del llamador) es 123456789, UNI-K necesite enviar 9123456789 a su troncal cuando llama a este número. Debería configurar el número 123456789 como el número de callback y agrega 9 antes de realizarse el Callback. Puede agregar "w" para troncales analógicos para una tardanza también.

6.7.5 Configuraciones de DNIS

DNIS (servicio de identificación de número marcado) es un servicio telefónico que identifica para el receptor de una llamada al número que marcó el llamador.

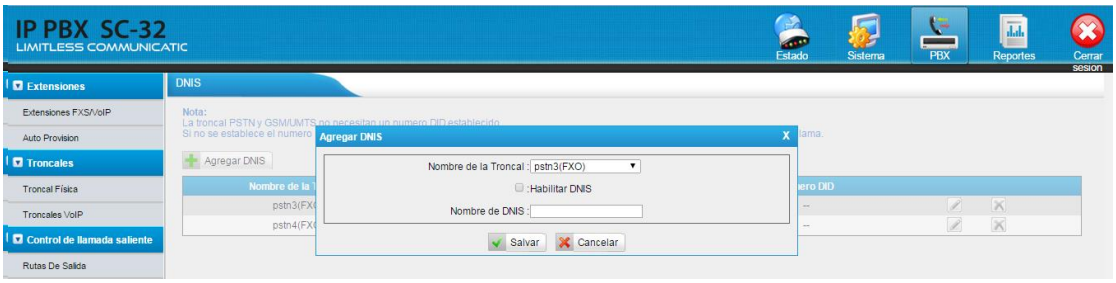


Figura 6-72

Nota: Si DID no se configura aquí, todas las llamadas vía este troncal muestran los DNIS en lugar de ID de llamador original.

6.7.6 DISA

DISA (Acceso Directo de Sistema Interno) permite que alguien llame desde afuera el switch telefónico (PBX) para obtener un tono de marcación "interna" del sistema y realizar llamadas como si estuvieran utilizando una de las extensiones conectadas al switch telefónico. Para utilizar DISA, un usuario llama un número DISA, que invoca la aplicación de DISA. La aplicación DISA a su vez

requiere al usuario que introduzca un número PIN, seguido por el signo de número (#). Si el número PIN es correcto, el usuario escuchará tono de llamada en la que se puede realizar una llamada. Obviamente, este tipo de acceso tiene implicaciones de seguridad graves, y debe tener mucho cuidado para no poner en peligro su seguridad.

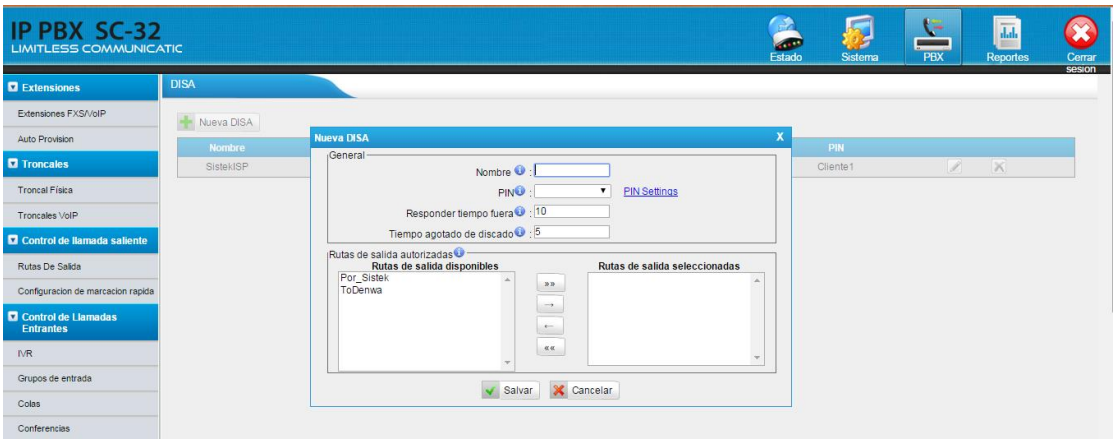


Figura 6-73

1) General

·Nombre de DISA

Da un nombre a esta aplicación DISA para ayudarle a identificarla.

·PIN

La contraseña para este DISA.

·Configuración de PIN

Haga clic para añadir, eliminar o editar lista de PIN.

·Respuesta de Tiempo Afuera

La cantidad máxima de tiempo el sistema esperará antes de colgar la llamada si el usuario ha marcado un número incompleto o inválido. El valor predeterminado es 10 segundos.

·Dígito de Tiempo Afuera

La cantidad máxima de tiempo permitido entre cada dígito cuando el usuario está marcando un número de extensión. El valor predeterminado es 5 segundos.

2) Miembro de Routes Salientes

Utiliza para establecer Routes salientes que se pueden acceder desde este DISA.

6.7.5 Configuraciones de PIN Usuario

PIN Usuario se utiliza para administrar listas de Pinos que pueden utilizarse para acceder a funciones restringidas tales como rutas salientes.

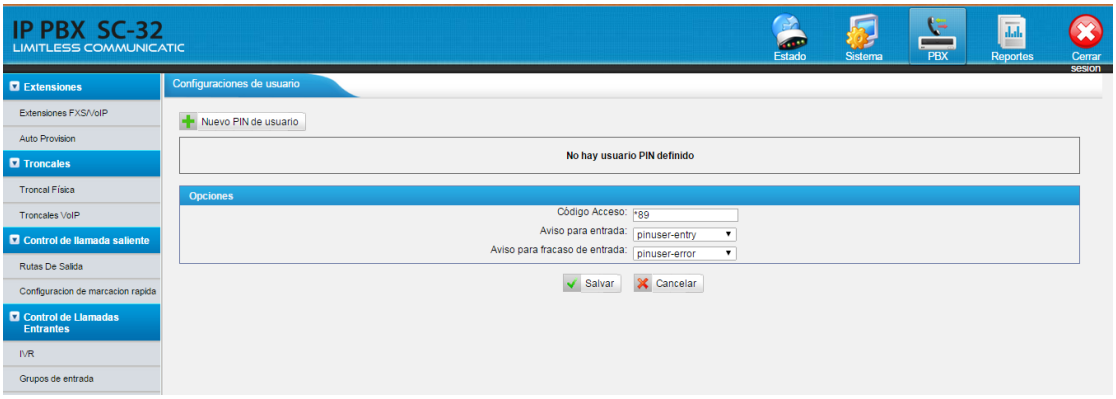


Figura 6-74

1) Opciones

·Código de Acceso

Marca este código para acceder PIN.

·Anuncio para Introduzca

Anuncia el llamador a introducir el número PIN.

·Anuncio para Introduzca Falla

Anuncia al llamador cuando un PIN inválido fue introducido.

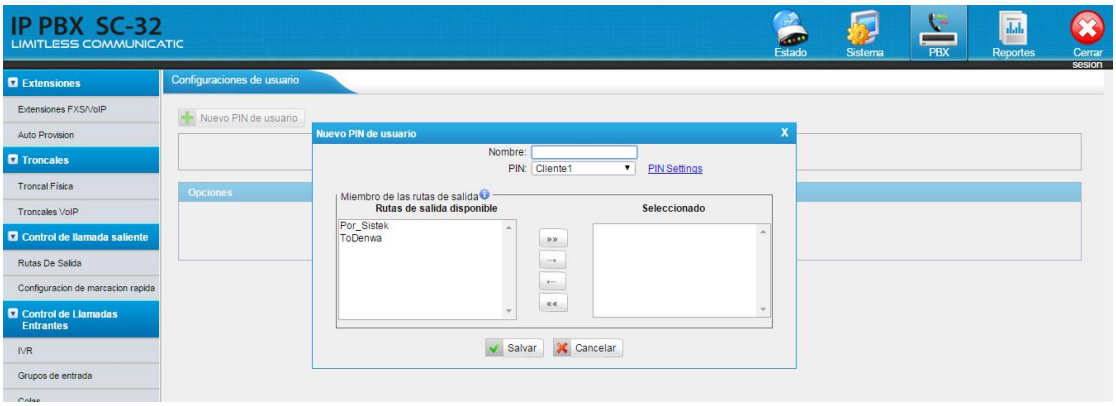


Figura 6-75

2) PIN Usuario

UNI-K puede almacenar un número de PIN usuarios. PIN usuarios pueden usarse para hacer un seguimiento de las llamadas en lo referente a actividades particulares o clientes. También puede ser utilizado para mantener un registro de llamadas por usuarios particulares o grupos de usuarios.

• PIN introducido se comprueba contra los almacenados por el sistema. Si se introduce un PIN inválido, el PIN se solicita otra vez.

• El administrador del sistema puede configurar ciertos números o tipos de números para requerir la entrada de un PIN antes de que los usuarios pueden seguir haciendo una llamada a tal un número.
• El administrador también puede configurar para tener que los usuarios puedan ingresar un PIN antes de hacer cualquier llamada externa.

·Nombre
Un nombre basados en caracteres para esta lista de PIN , por ejemplo "SISTEKPIN"

·PIN
La contraseña para esta lista de PIN

·Configuración de PIN
Haga clic para añadir, eliminar o editar lista de PIN.

·Miembro de Route Saliente
PIN Usuario puede utilizar los route salientes a hacer llamada a afuera.

6.7.8 Configuraciones de PIN

En esta página los usuarios pueden administrar todas las contraseñas de routes salientes, PIN Usuario, y DISA.

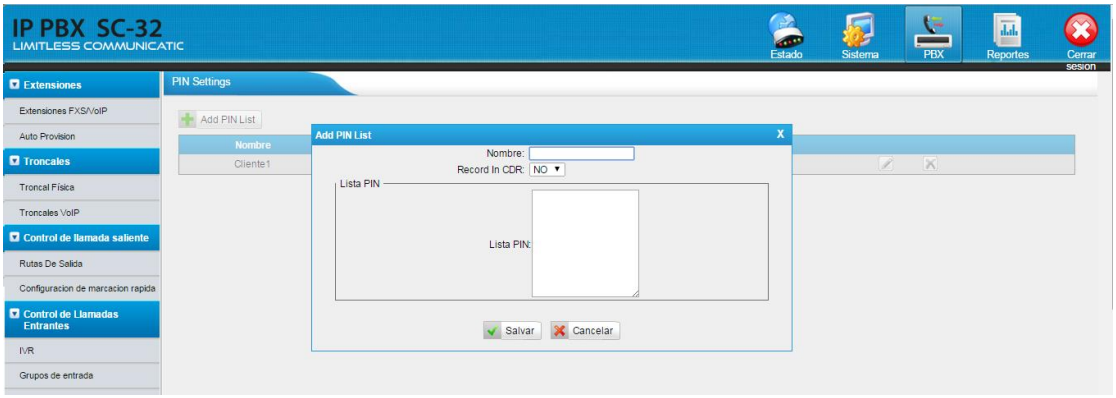


Figura 6-76

·Nombre
Un nombre basados en caracteres para esta lista de PIN , por ejemplo "SISTEKPIN"

·Grabar en CDR
Si establece en sí, el PIN código reproducirá en registro de llamada.

·Lista de PIN

La lista de PIN es un campo numérico. No se permiten letras y puntuación en este campo.

Rellene un PIN y si termina con la tecla "entre" para cada PIN, puede crear múltiples pasadores.

6.7.9 Grupos de Paging

La paging se utiliza para hacer un anuncio sobre el altavoz a un teléfono o un grupo de teléfonos. Los teléfonos no sonará, pero en cambio responder inmediatamente en el modo de altavoz. Por favor tenga en cuenta que esta sección es para configurar grupos de paging. Si desea configurar la intercomunicación, por favor abra la Otras Configuraciones-> Códigos de Función.

Esta función es soportada por los siguientes teléfonos SIP:

Yealink's T28, T26, T22, T20, T10T, T9CM. Otros dispositivos SIP también pueden funcionar con esta función, pero oficialmente no son soportados.

Nota: Un grupo paging puede tener máximamente de 20 miembros

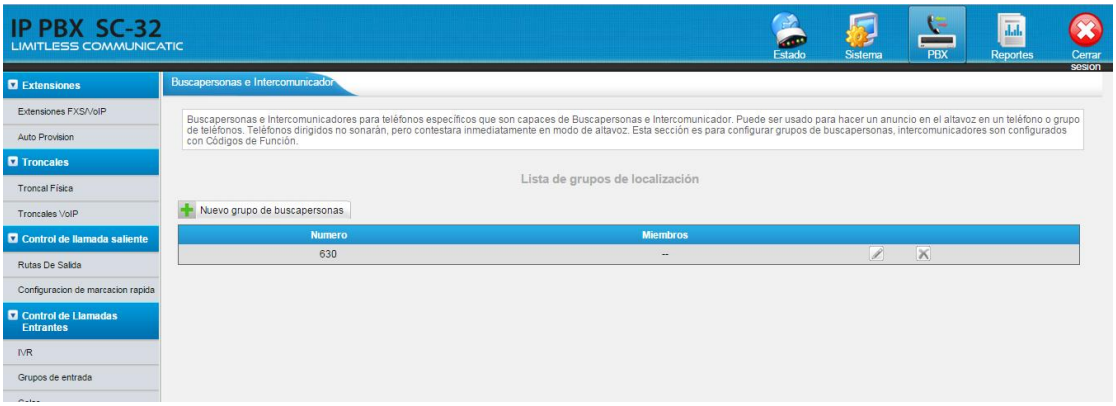


Figura 6-77

En este modo, si usted marcar su número, UNI-K ayudará a recoger esos miembros elegidos y puede hablar directamente sin ningún sonidos.

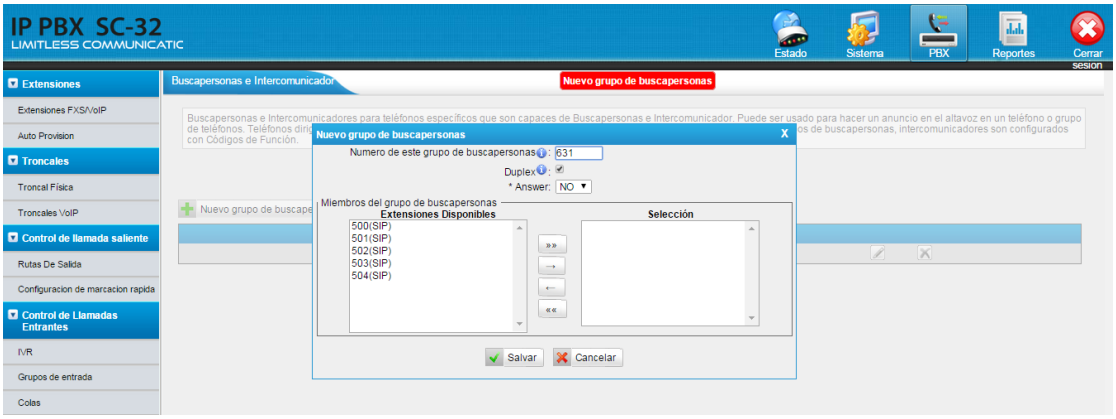


Figura 6-78

·Número del Grupo Paging

Define el número de extensión que puede ser marcado para alcanzar este grupo.

·Dúplex

Paging es típicamente una forma solamente para los anuncios. Comprueba esto hará que la paging dúplex, permitiendo que a todos los usuarios del grupo para hablar y ser escuchado por todos.

·*Contesta

Si es establecido en Sí, algunos usuarios en el grupo hablarán con el llamador cuando ellos presionen "*". Si es establecido en No, los usuarios en el grupo puede hablar uno con el otro sin presiona "*".

6.7.10 Certificados

UNI-K puede soportar TLS extensión. Antes de registrarse la extensión TLS en teléfono IP, usted debe cargar primero certificados.

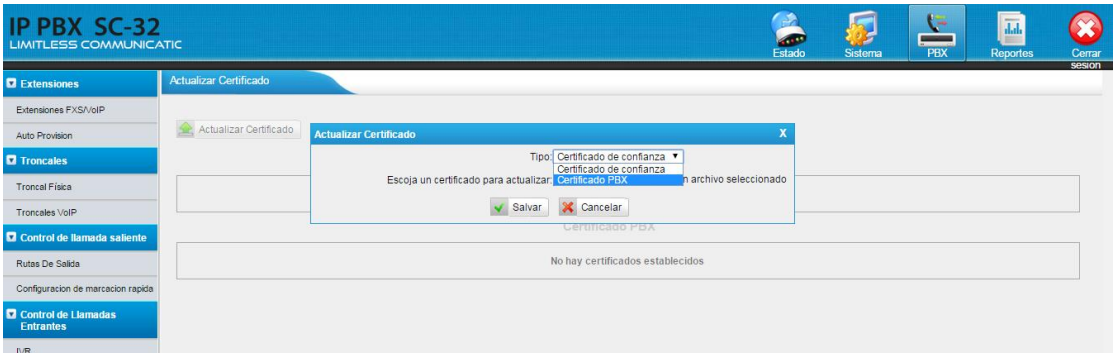


Figura 6-79

Certificado Confiado

Este certificado es un CA certificado. Cuando seleccione "TLS Verifique Cliente" como "sí" , puede cargar un CA. El teléfono IP relacionado debería también tener certificado.

PBX Certificado

Este certificado es un servidor certificado. No importa si seleccione "TLS Verifique Cliente" como "sí" o "NO", debería cargar este certificado a UNI-K. Si

el teléfono IP habilitó "TLS Verifique Cliente", deberá también cargar CA certificado correspondiente en teléfono IP.

7. Reportes

Haga clic en

para accederse.

Podemos comprobar los registros detallados de llamadas para contabilización y registro del sistema para la depuración.

7.1 Registros de Llamada

El Registro de llamada captura todos los detalles de la llamada, incluyendo tiempo de llamada, número de llamador, número destinatario, tipo de llamada, duración de la llamada, etc.. Un administrador puede buscar y filtrar datos de llamada por fecha de llamada, llamador/destinatario, troncal, duración, duración de tarifación, estado, tipo de comunicación y usuario de PIN.

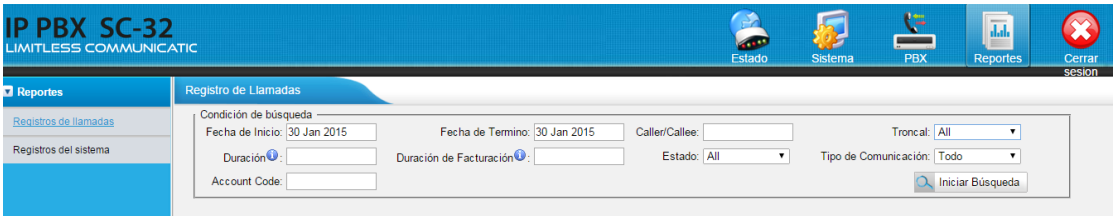


Figura 7-1

7.2 Registros de Sistema

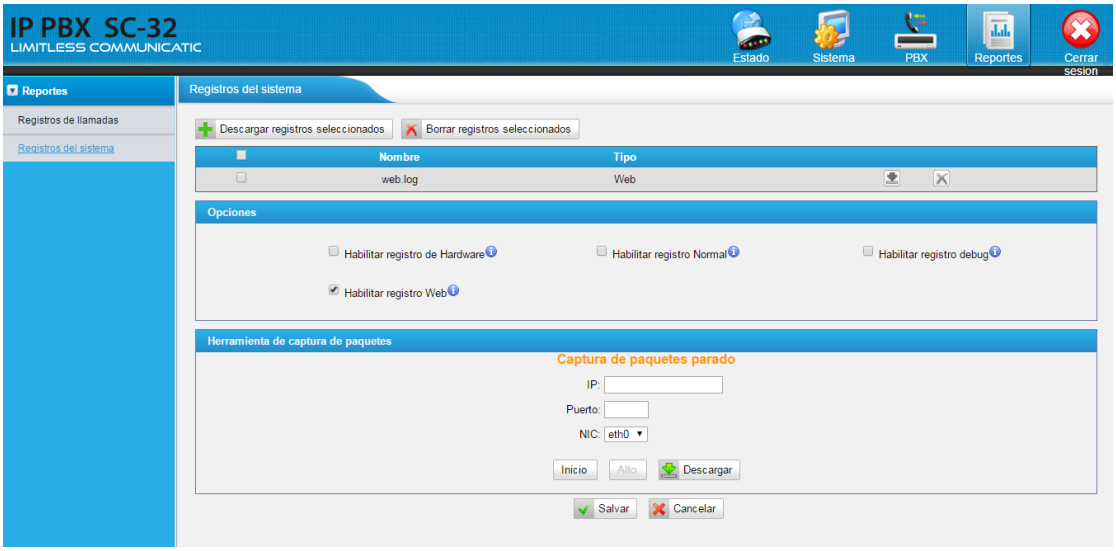


Figura 7-2

Puede descargar y eliminar los registros de sistema de UNI-K.

Opciones

·Habilita Registro de Hardware

Guarda la información del hardware; (hasta 4 archivos de registro)

·Habilita Registro Normal

Guarda la información del anuncio; (hasta 16 archivos de registro)

·Habilita Registro de Web

Guarda la historia de operaciones de web; (hasta 2 archivos de registro)

·Habilita Registro Depuración

Guarda la información depuración; (hasta 2 archivos de registro)

Herramienta de Paquetes Captura

Esta funcionalidad es utilizada por técnico a capturar paquetes. La herramienta de captura de paquetes "Wireshark" está integrada en UNI-K.

Los usuarios también pueden especificar la dirección IP de destino y el puerto a obtener los paquetes.

·IP

Especifique la dirección IP de destino para obtener los paquetes.

·Puerto

Especifique el destino de Puerto para obtener los paquetes.

·NIC
Elija la NIC (LAN o WAN) que desea capturar los paquetes.

8. Logout

Haga clic en

para cerrar la sesión de forma segura..

9. Use UNI-K

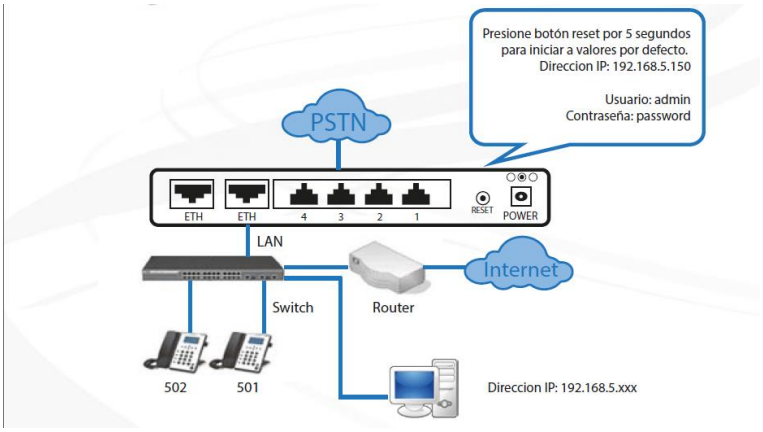


Figura 9-1

9.1 Hacer Llamadas Salientes

Para hacer una llamada saliente, deberemos agregar al troncal primero. Hay 3 tipos de troncal VoIP.
·VOIP Troncal: Conecta al servidor de VOIP servicio remoto.
Debería obtener una dirección IP con nombre de usuario/contraseña desde el proveedor.
·Proveedor de Servicio: Conecta al servidor de VoIP servicio.
Conseguirá solamente la dirección IP para la autorización.
·Troncal Analógico: Los puerto FXO de UNI-K, conecta a PSTN local.

·**Troncal BRI:** Los puertos BRI de UNI-K, conecta a ISDN proveedor.

¿Qué son FXO y FXS?
FXS (Foreign Exchange Station) es un interfaz que conduce un teléfono analógico o máquina FAX. Interfaces FXS alimenta energía, proporcionan sonido y utilizan señalización FXO. Interfaces FXS son lo que le permiten conectar teléfonos y otros dispositivos analógicos a su PBX.
FXO (Foreign Exchange Office) es una interfaz que se conecta a una línea telefónica para suministrar su PBX con acceso a una red pública de telefonía. Interfaces FXO utilizan señalización FXS. Interfaces FXO permiten que usted conecte su PBX con líneas teléfonos analógicos reales.

Ejemplo de Enrutamiento vía Troncal VoIP

Vamos a configurar todas las extensiones internas a marcar "0" a través de Troncal VoIP.

1. Añadir Proveedor de VoIP Servicio

Antes de añadir este, por favor asegúrese que tiene una cuenta de Troncal VoIP.
Troncales→VoIP Troncal →SIP Troncal
Ingrese la información de su cuenta en esta página, y haga clic a guardar.

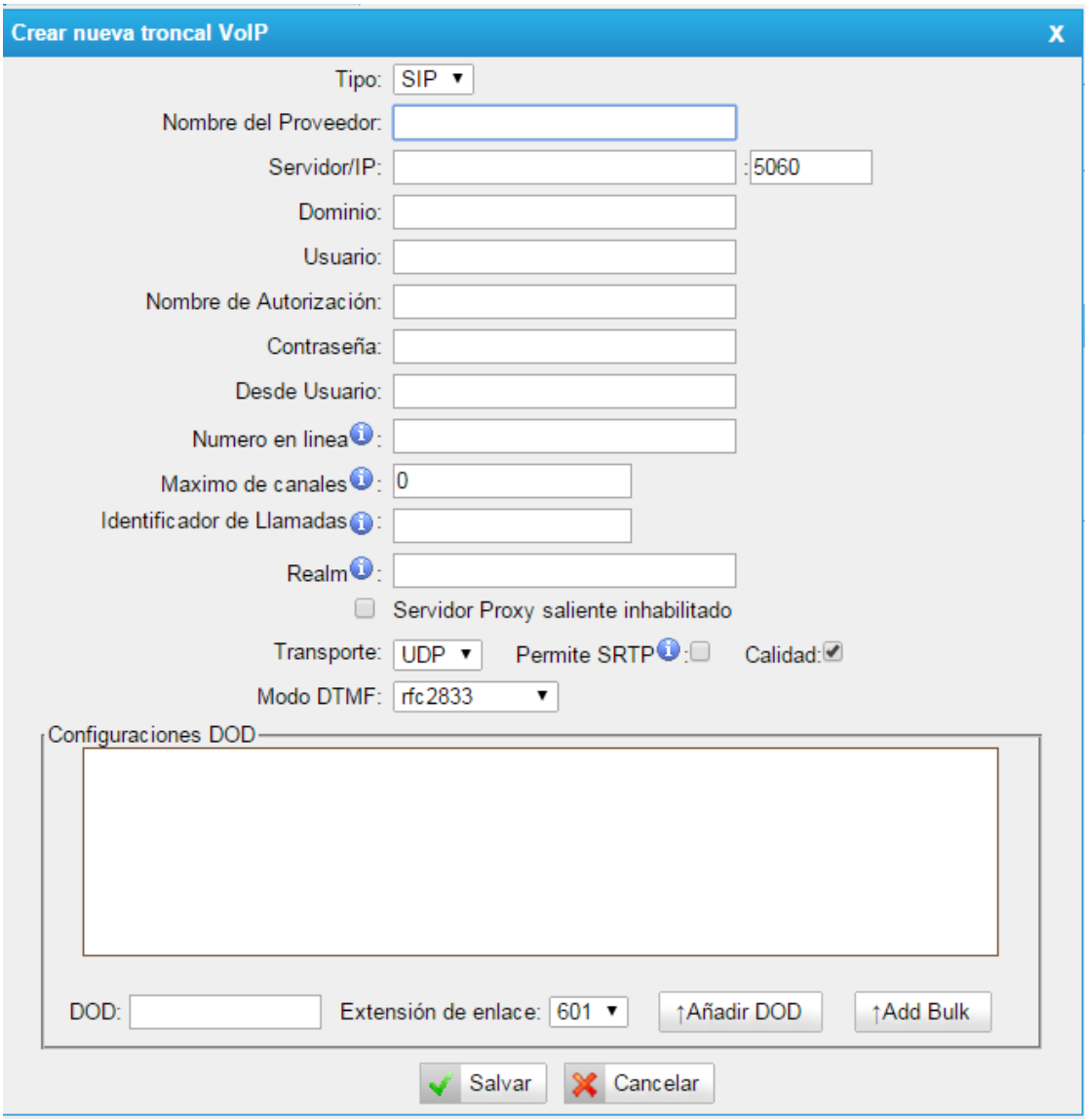


Figura 9-2

2. Añadir Rutas Salientes

Como podemos ver desde la ruta saliente de "VOIP_OUT", todos los números telefónicos que iniciando con 0 tendrán sus dígitos primeros quitados (dígito 0) y será enviado a Troncal SIP.

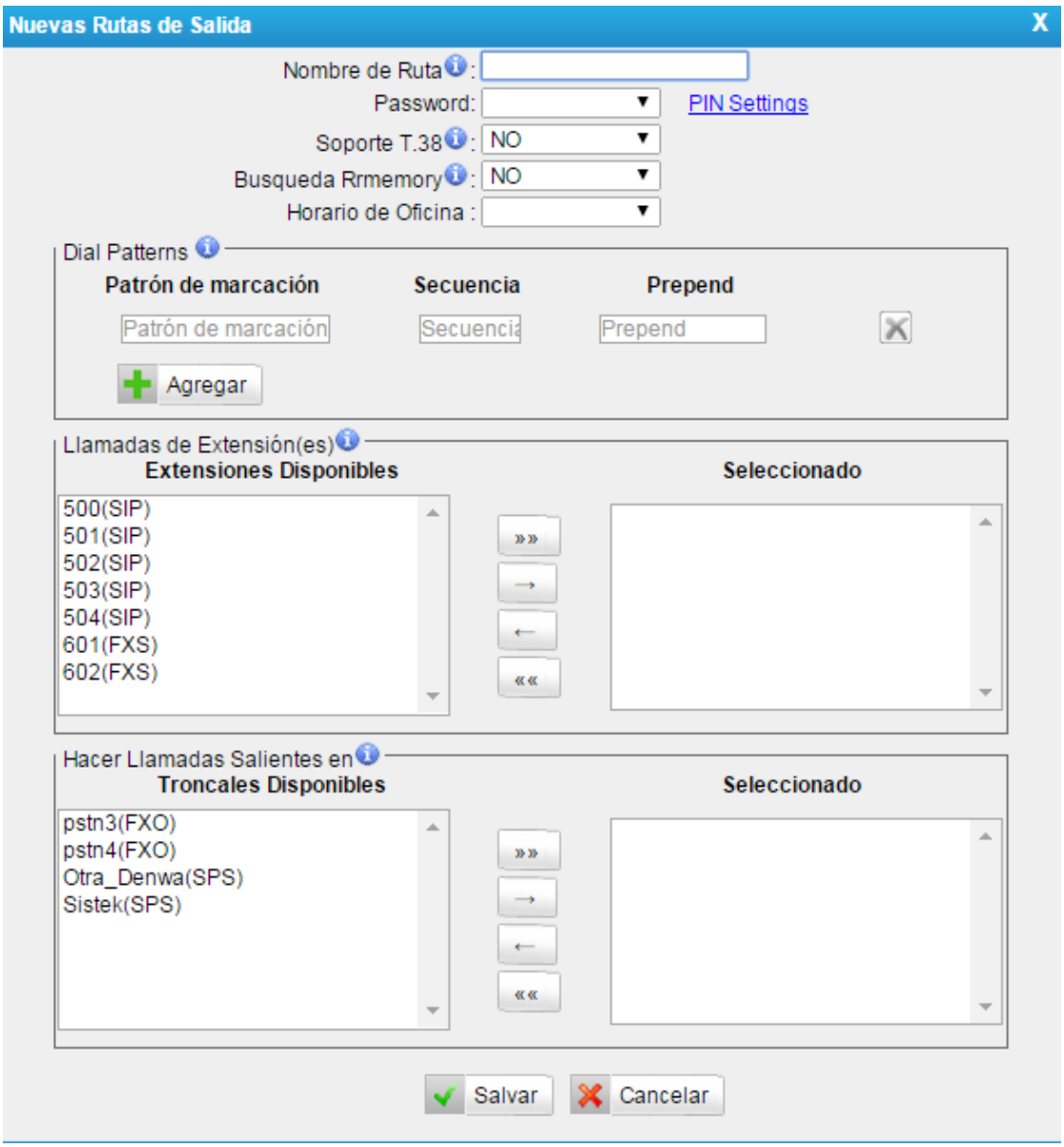


Figura 9-3

Ahora que agregábamos dos reglas de marcado saliente, unas llamadas iniciando con 9 serán rutadas a PSTN y unos números iniciando con 0 serán rutados a Troncal SIP.

9.2 Llamada Entrante

Ejemplo de Enrutamiento a un IVR

Vamos a configurar una llamada entrante a enrutar a IVR. En el IVR de sí mismo, vamos a configurar dígito 0 para enrutar la llamada a la extensión 300 y dígito 1 para enrutar la llamada a grupo de sonido.

1. Añadir IVR

Para añadir un nuevo IVR, visitar IVR→ Crear IVR Nuevo

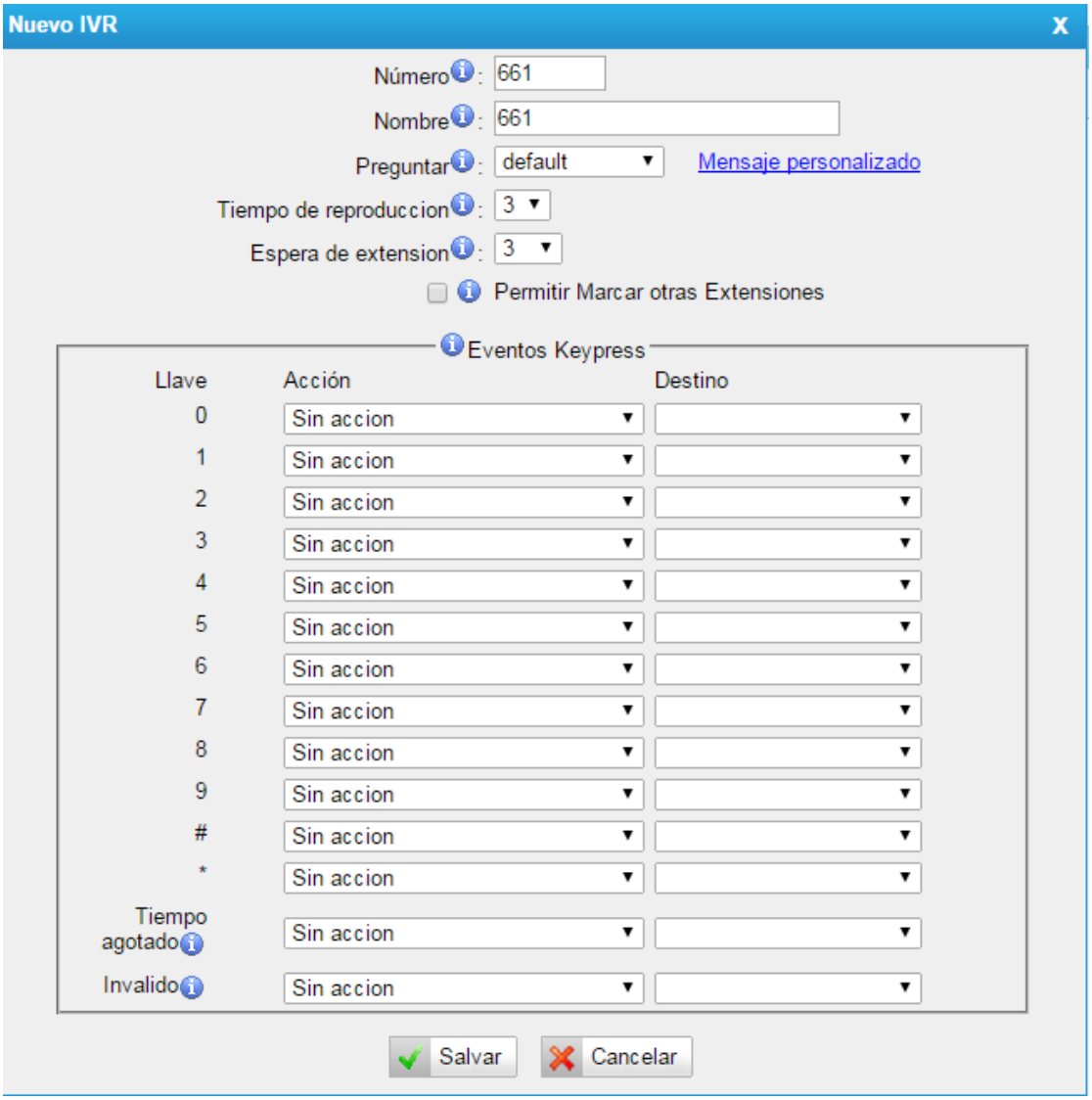


Figura 9-4

2. Añadir Rutas Entrantes

Como podemos ver desde la Ruta Entrante de "VOIP_IN", todas las llamadas entrantes vienen de troncal VoIP serán enviadas a IVR.

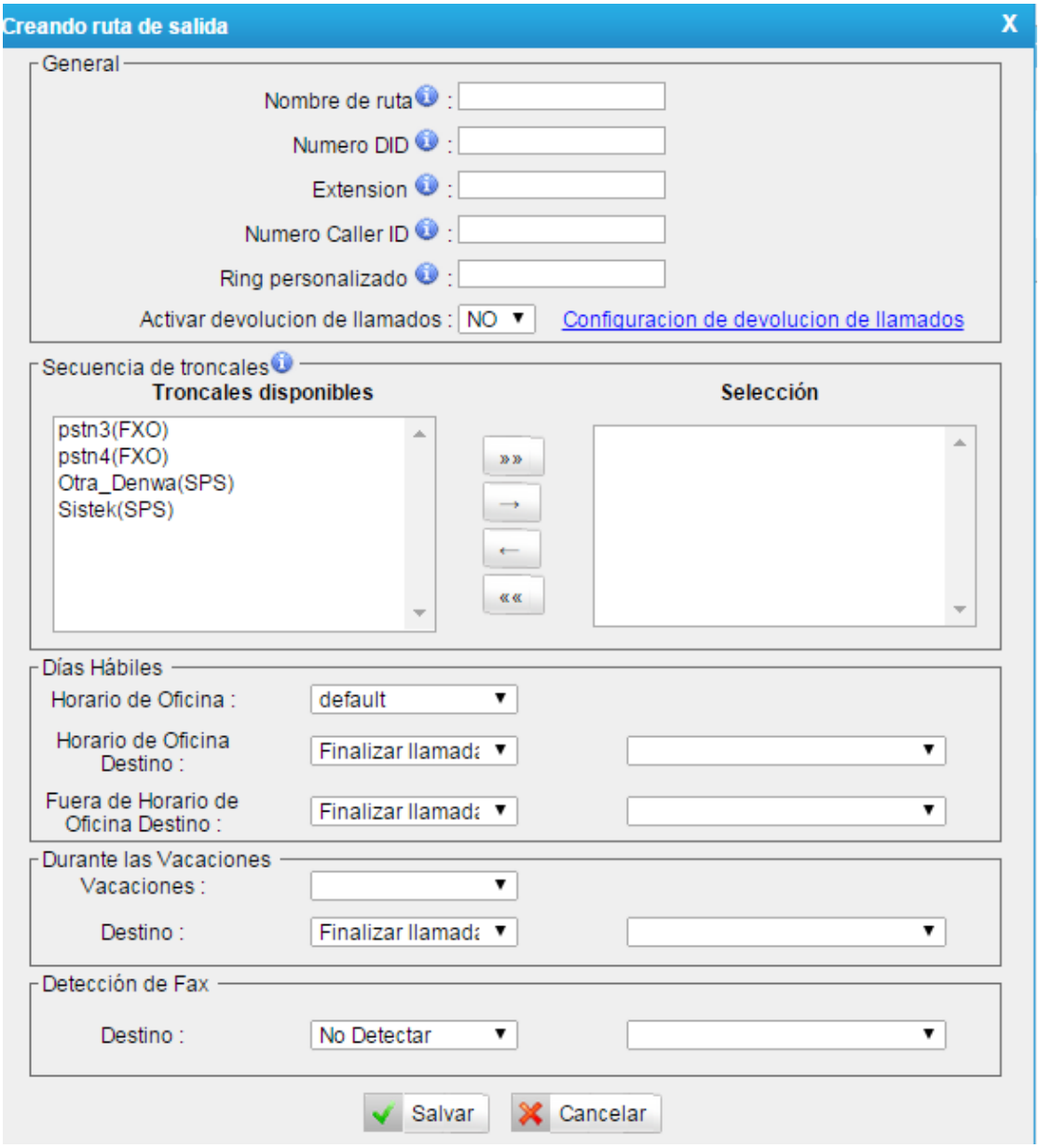


Figura 9-5

APPENDIX A FAQ

Q1. ¿Cómo Registra Dispositivos SIP?

A1:
1) Registro SIP soft phone
Descarga el x-lite softphone desde la página web CounterPath
www.counterpath.com
Después de la instalación del x-lite, haga clic en el panel y selecciona Configuración de Cuenta SIP y luego la configura.
Nombre Mostrado: 500
Nombre de Usuario: 500
Contraseña: 500
Autorización del nombre 500
Domain 192.168.5.150

2) Registro de Teléfono IP (Por ejemplo, Teléfono IP T28 de Yealink)
a) Conecta puerto del Internet de T28 al switch. Y puede obtener la IP desde su route
b) Presiona la tecla "OK" en T28 para obtener la IP de T28.
c) Pone la IP en el web navegador y puede ingresar la página de configuración de T28 a través de esta IP.
d) Pone la información de las extensiones SIP en el teléfono IP T28.
Nombre Mostrado: 501
Nombre de Usuario: 501
·Nombre Registro: 501
Contraseña: 501
Servidor SIP: 192.168.5.150
aplica el mismo método de registro a otro T28 para otra extensión.

Q2. ¿Cómo puedo restablecer UNI-K a las Configuraciones predeterminadas de Fábrica?

A2: Para realizar un restablecimiento, por favor sigue los pasos de abajo:
Paso 1: Mantenga pulsado el botón "Reset" en la parte posterior de la unidad durante 5 segundos y ver los LEDs en la parte frontal de la UNI-K. Cuando el LED

se enciende rojo, suelte el botón de restablecimiento.

Paso 2: Cuando empiece a parpadear el LED de funcionamiento, UNI-K se establecerá devuelta a los valores predeterminados de fábrica.

Paso 3: Para acceder a la página de configuración, se navega a 192.168.5.150 utilizando un navegador de web. Asegurase que está en suben de 192.168.5.0 antes de hacerlo.

Paso 4: Ingrese en el dispositivo con el nombre de usuario "admin" y la contraseña "password" y volver a configurar el dispositivo.

APPENDIX B ¿Cómo configura Almacenamiento Externo?

Antes del almacenamiento externo puede ser configurado correctamente, una carpeta compartida accesible de SMB desde UNI-K debe configurarse en un equipo basado en Windows. Una vez que han sido configurados, por favor sigue los pasos siguientes.

Paso 1 Agrega una carpeta nueva, cámbiele el nombre y parte de las Propiedades esta carpeta nueva según la figura B-1.

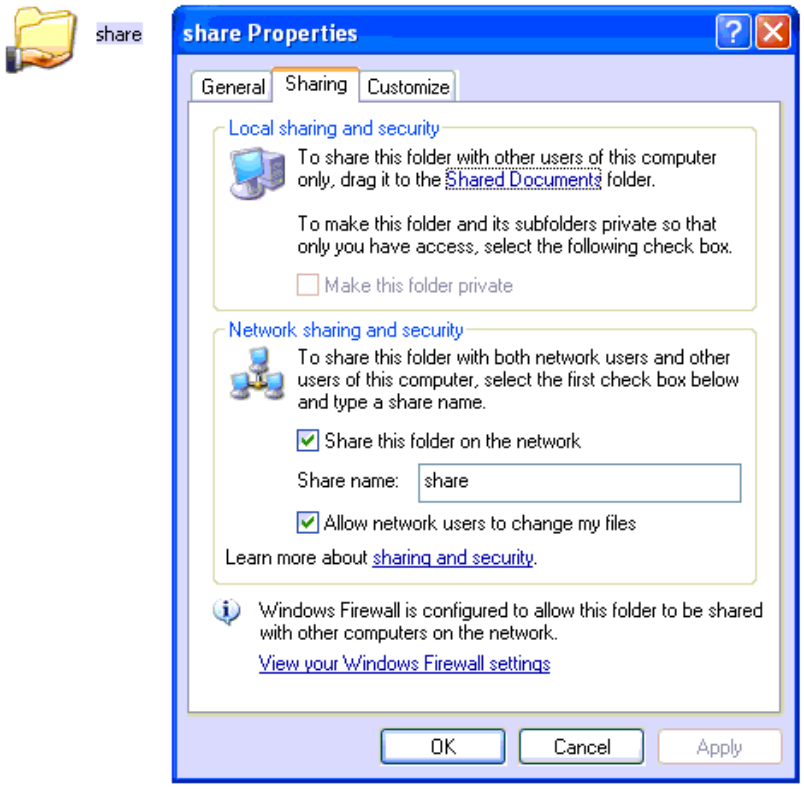

share
share Properties
General
Sharing
Customize
Local sharing and security
To share this folder with other users of this computer only, drag it to the Shared Documents folder.
To make this folder and its subfolders private so that only you have access, select the following check box.
Make this folder private
Network sharing and security
To share this folder with both network users and other users of this computer, select the first check box below and type a share name.
Share this folder on the network
Share name: share
Allow network users to change my files
Learn more about sharing and security.
Windows Firewall is configured to allow this folder to be shared with other computers on the network.
View your Windows Firewall settings
OK
Cancel
Apply

Figura B-1 Configura Propiedades Compartidas

Paso 2 Ingrese en la carpeta nueva y crea un archivo nuevo de texto, luego cambie este archivo a status.txt este paso es muy importante, no se olvide de crear el archivo status.txt

Paso 3 Configura las opciones de almacenamiento externo en UNI-K según figura B-2.

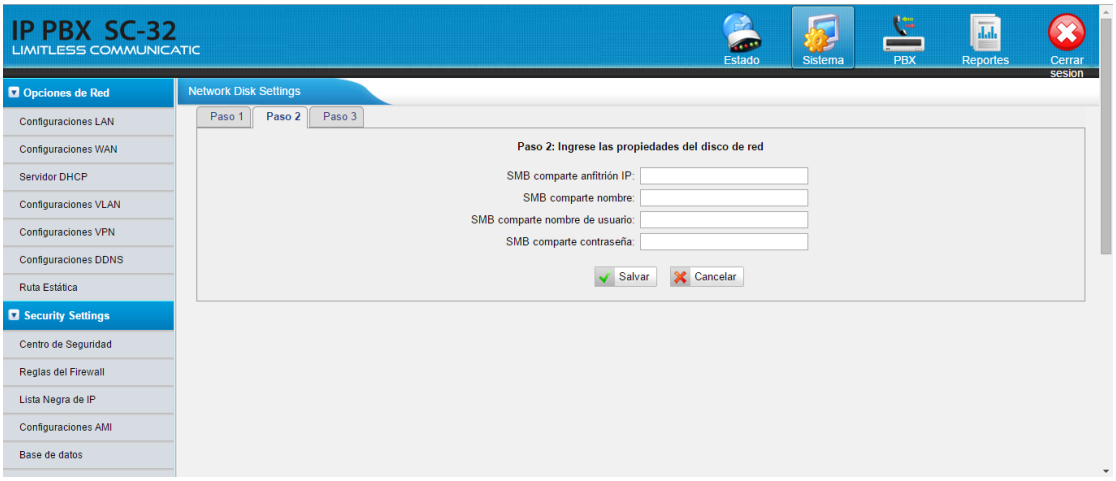


Figura B-2 Configuración del Almacenamiento Externo

Host/IP del Net-Disco: Cambie esto a la dirección IP de la computadora en dónde se almacenarán los archivos de copia de seguridad.

Nombre del Net-Disco Compartido: Cambie esto al nombre de la carpeta compartida en dónde se almacenarán las copias de seguridad.

Nombre del Usuario del Net-Disco Compartido: El nombre del usuario se utiliza para registrarse en la red compartida. Dejase en blanco si no lo requiere.

Contraseña del Net-Disco Compartido: La contraseña se utiliza para registrarse en la red compartida. Dejase en blanco si no lo requiere.

Abre la carpeta compartida de su Windows para ver si los archivos de copia de seguridad y carpeta habían sido creados. Si el contenido de la carpeta de copia de seguridad tienen un aspecto similar a la Figura B-3, entonces ha configurado correctamente el almacenamiento externo de la unidad UNI-K.

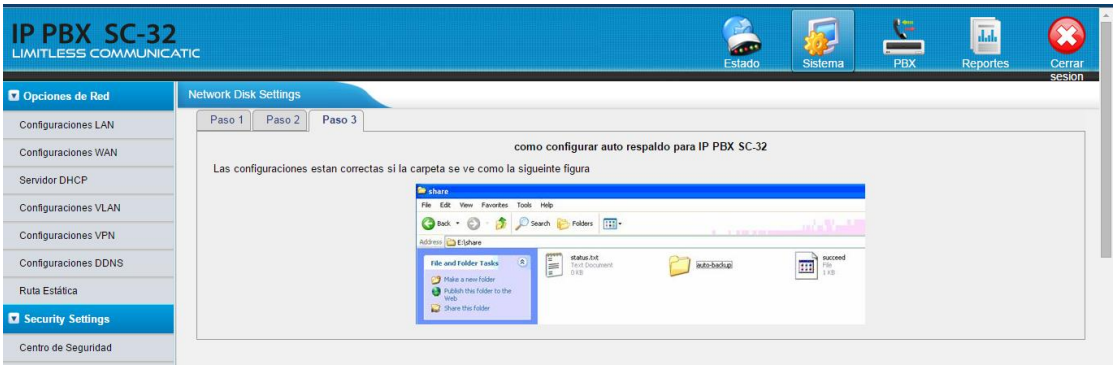


Figura B-3 Configuración del Almacenamiento Externo con éxito

APPENDIX C ¿Cómo Configura NAT?

Cuando UNI-K está detrás de un NAT (firewall), tiene que configurar NAT en UNI-K si desea utilizar una extensión remota.
Por favor siga en la sección 1 o 2 abajo dependiendo de su configuración de red.
1. Si UNI-K está conectado a una red local, debe configurar un puerto de reenvío en tu router. Especialmente, debe asignar puertos 5060 (puerto SIP predeterminado) y Puerto 10001-10200(Rango de puertos de RTP predeterminado) como puertos UDP.

A continuación, ingrese en Web GUI de UNI-K, vaya a "PBX"->"Configuraciones Avanzadas" ->"Configuraciones de SIP" -> "NAT"
Dirección IP Externa: Dirección IP pública del router suyo
Host Externo: Domain del router suyo
Intervalo de actualización externo: 20 segundos
Identificación de Red Local:192.168.5.0/255.255.255.0 (cambia este correspondiendo a la configuración de su Red)
NAT modo: Sí
Permite RTP Re invite: Sí

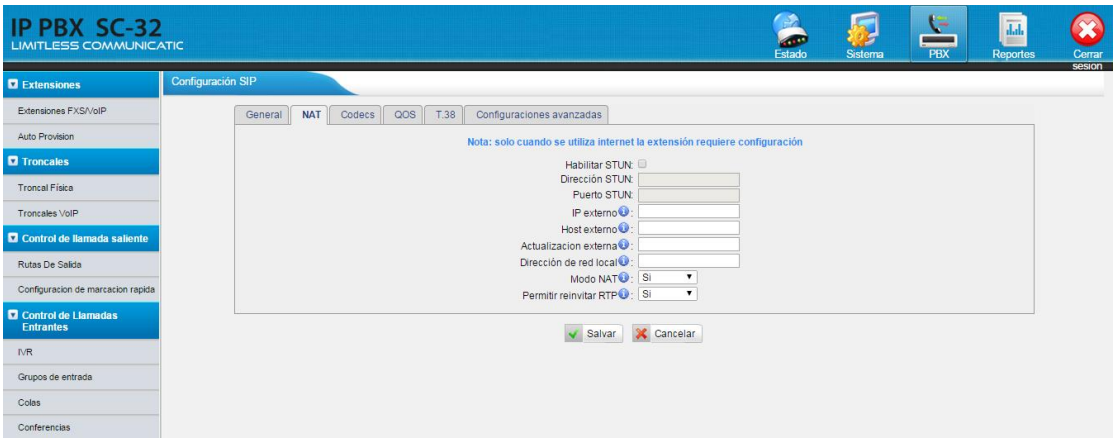


Figura C-1

Suponiendo que la dirección del host de su router es SISTEK.3322.org, su red local es de 192.168.5.1-192.168.5.254, y la máscara de suben es 255.255.255.0, la configuración de red de UNI-K debe configurada como Figura C-2.

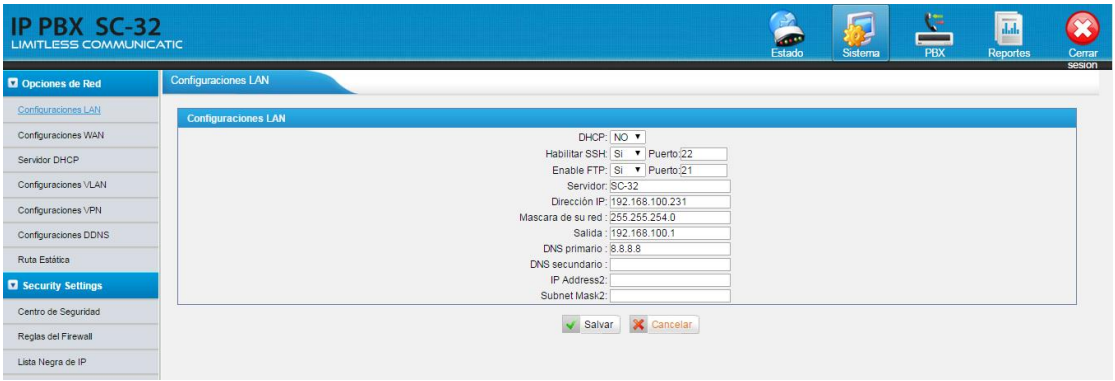


Figura C-2 Configuración de Red de UNI-K

2. Si UNI-K tiene una IP pública (es decir, se conecta directamente a su proveedor de internet), la configuración de red debe configurarse según figura C-3:

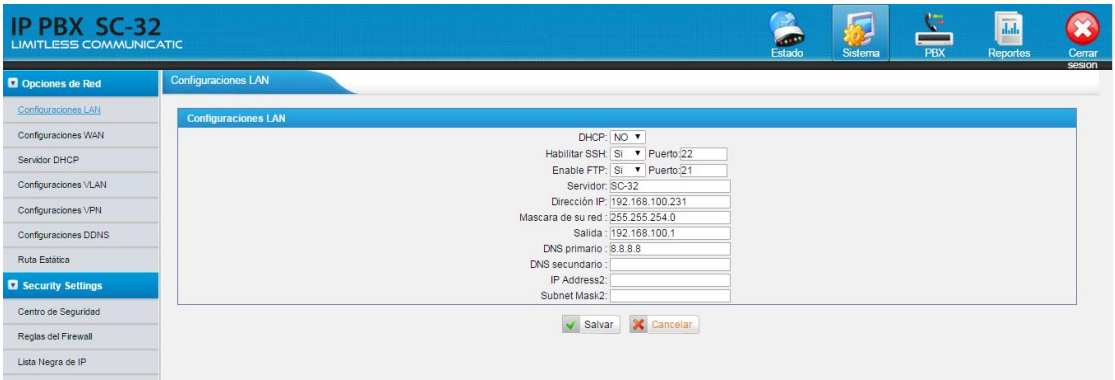


Figura C-3

Ahora, UNI-K se ha configurado como una IP pública, entonces no hay necesidad a configurar NAT otra vez, dejan todos los ajustes en el "NAT" en blanco.

APPENDIX D ¿Cómo Utiliza Auto Provisión?

Paso 1. Desactiva Servidor DHCP en su red local.
Por ejemplo Desactiva Servido DHCP en Router Linksys.

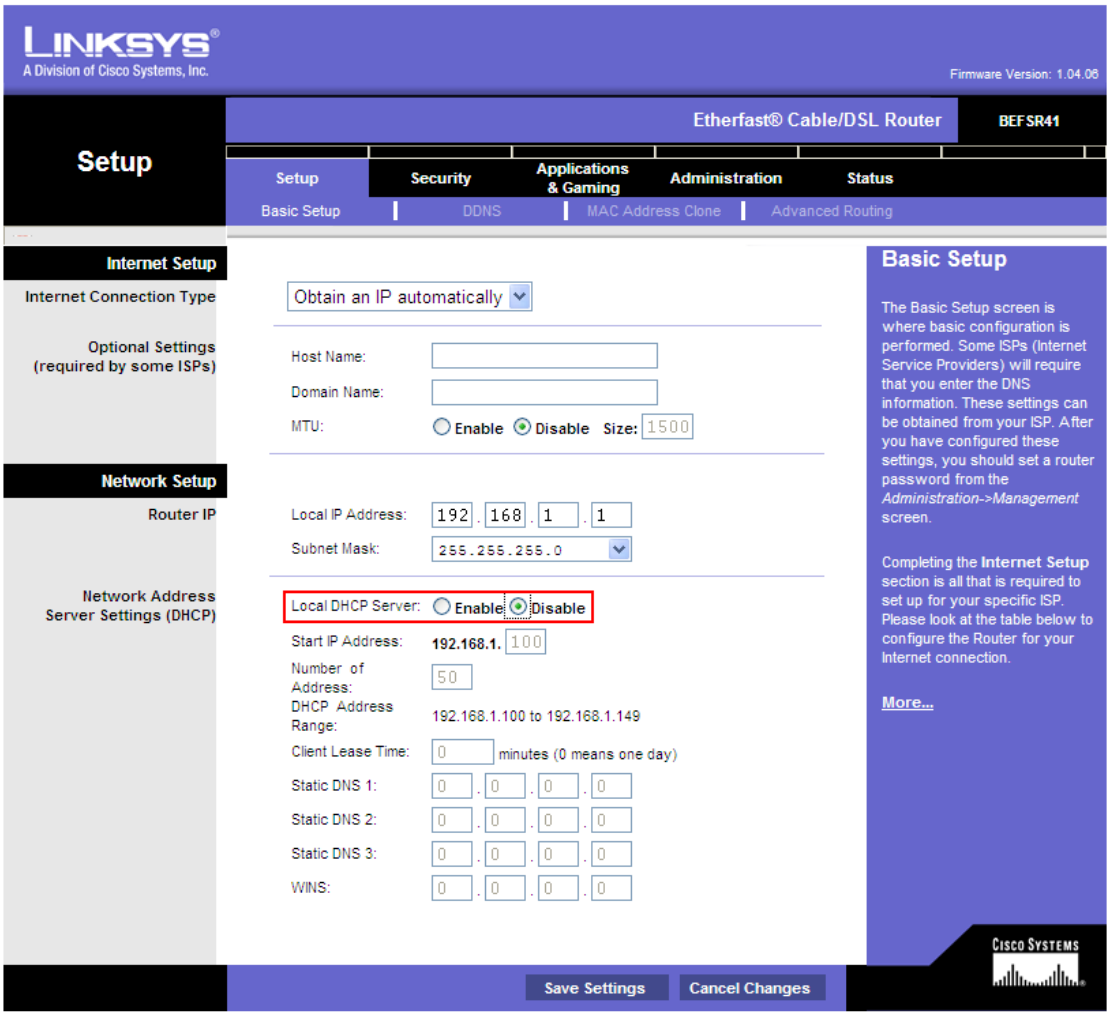


Figura D-1

Paso 2. Desactiva Servidor DHCP en UNI-K.

Ingrese web interfaz de UNI-K, "Sistema"→"Preferencias de Red" ->"Servidor DHCP"→"Desactiva Servidor DHCP".

Figura D-2

Paso 3. Configura teléfonos en la página auto provisión de UNI-K.

1. Ingrese web interfaz de UNI-K, "PBX" ->"Extensiones" ->"Teléfono Provisión" ->"Añadir Teléfonos".

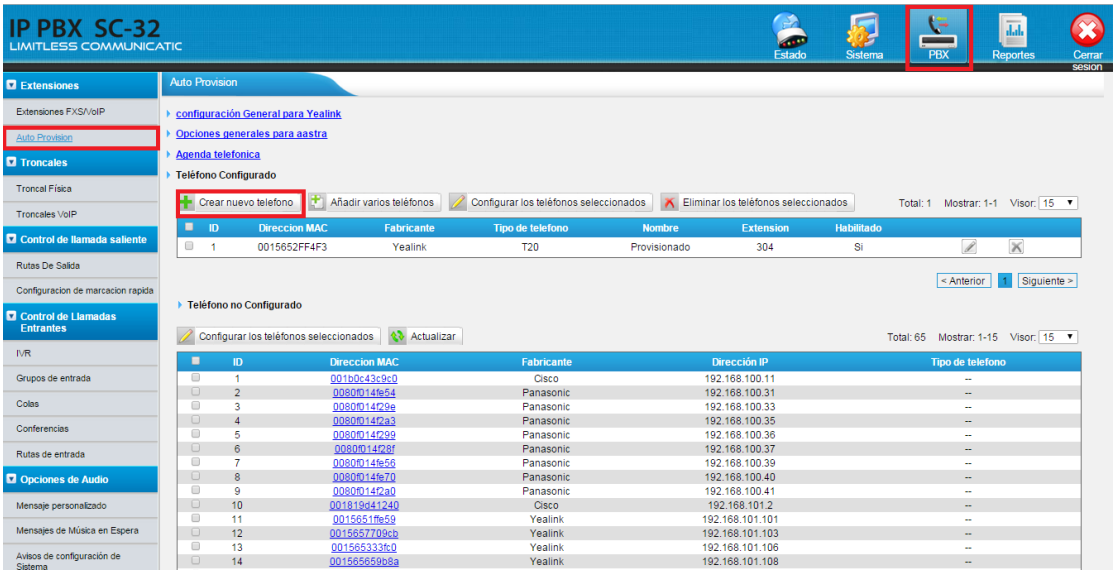


Figura D-3

2. Rellene detalle del mensaje telefónico en las ventanas emergentes.

Introducen la dirección MAC del teléfono IP, Nombre configurado, llamada en espera, línea, extensión, etiqueta, línea activa para el teléfono. Y también se pueden configurar otras características en el teléfono, como códigos, llaves de memoria etc..

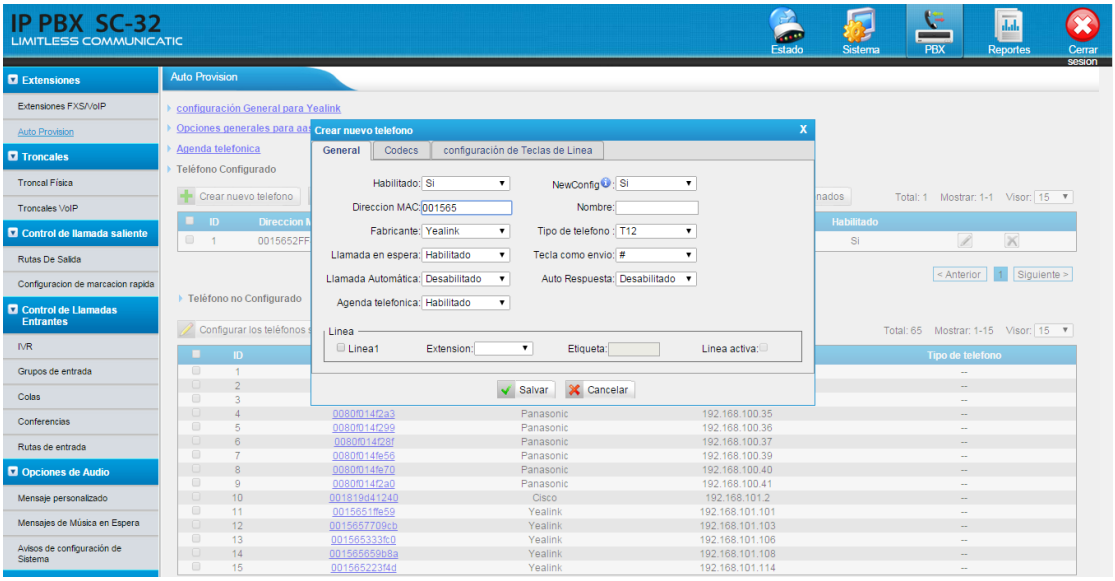


Figura D-4

Paso 4. Enciende la energía y conecte el cable de red al teléfono IP.

Nota: La configuración de fábrica de DHCP para teléfono IP está habilitada, así que puede saltarse este paso a paso 5.

Si el DHCP está desactivado, por favor siga los pasos de abajo para activarlo (por ejemplo Teléfonos IP de Yealink).

1. Ingrese página Web de teléfono IP.
2. Activa DHCP.

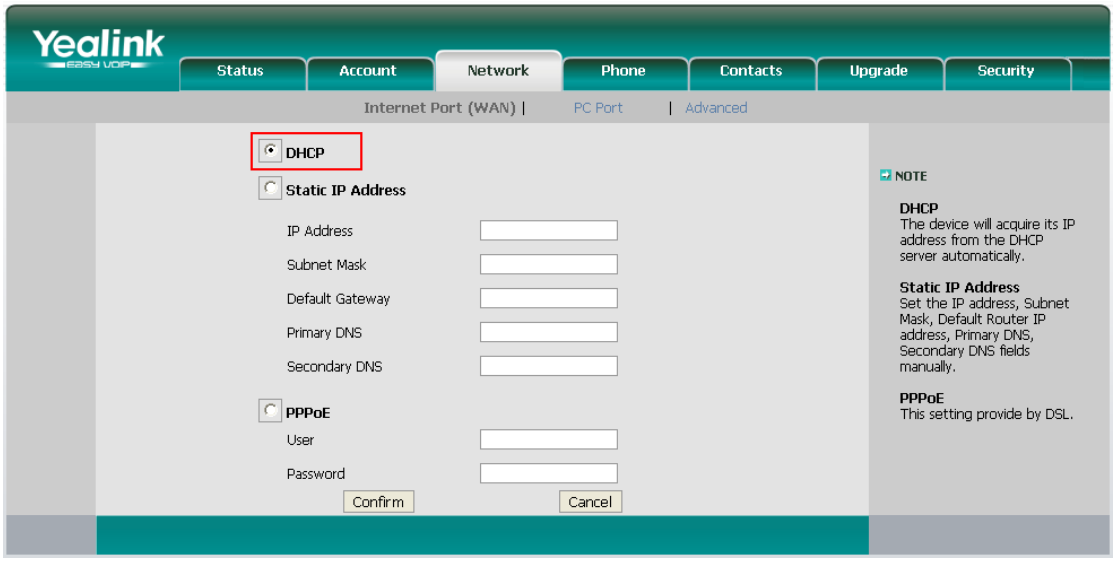


Figura D-5

Paso 5. Final.

APPENDIX E ¿Cómo Puedo Configurar los Tonos Distintivos?

Paso1: En el teléfono IP, navega a la página de configuración de teléfono de web configuración y encuentra la sección de tono de timbre distintivo.
Para cada tono de timbre personalizado, introduzca el texto de timbre interno (pueden ser números o texto) para activar el tono de timbre. Por ejemplo, puede introducir "Familiar".
Por ejemplo, teléfono IP de Yealink.

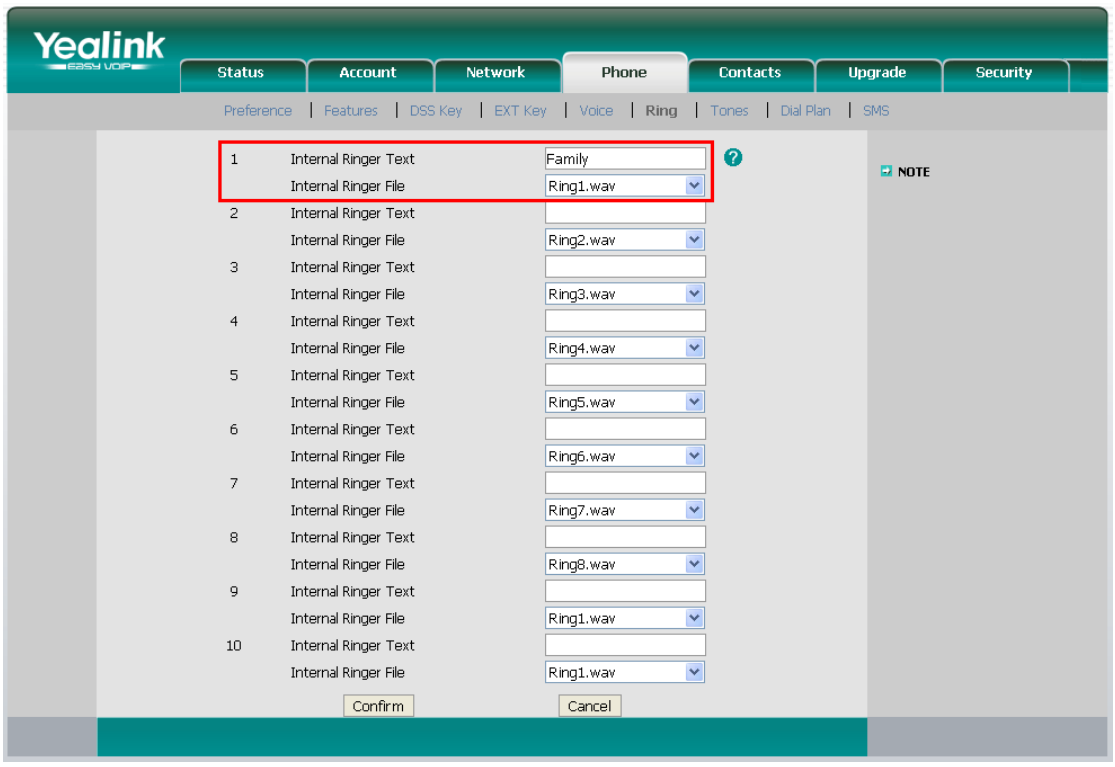


Figura E-1

Paso 2. Configura el "Tono distintivo" en UNI-K.
Ingrese en UNI-K web interfaz, "PBX"-> "Control de llamadas entrantes"-> "Routes Entrantes" → Editar Route Entrante, rellene el texto de Timbre Interno "Tono Distintivo".

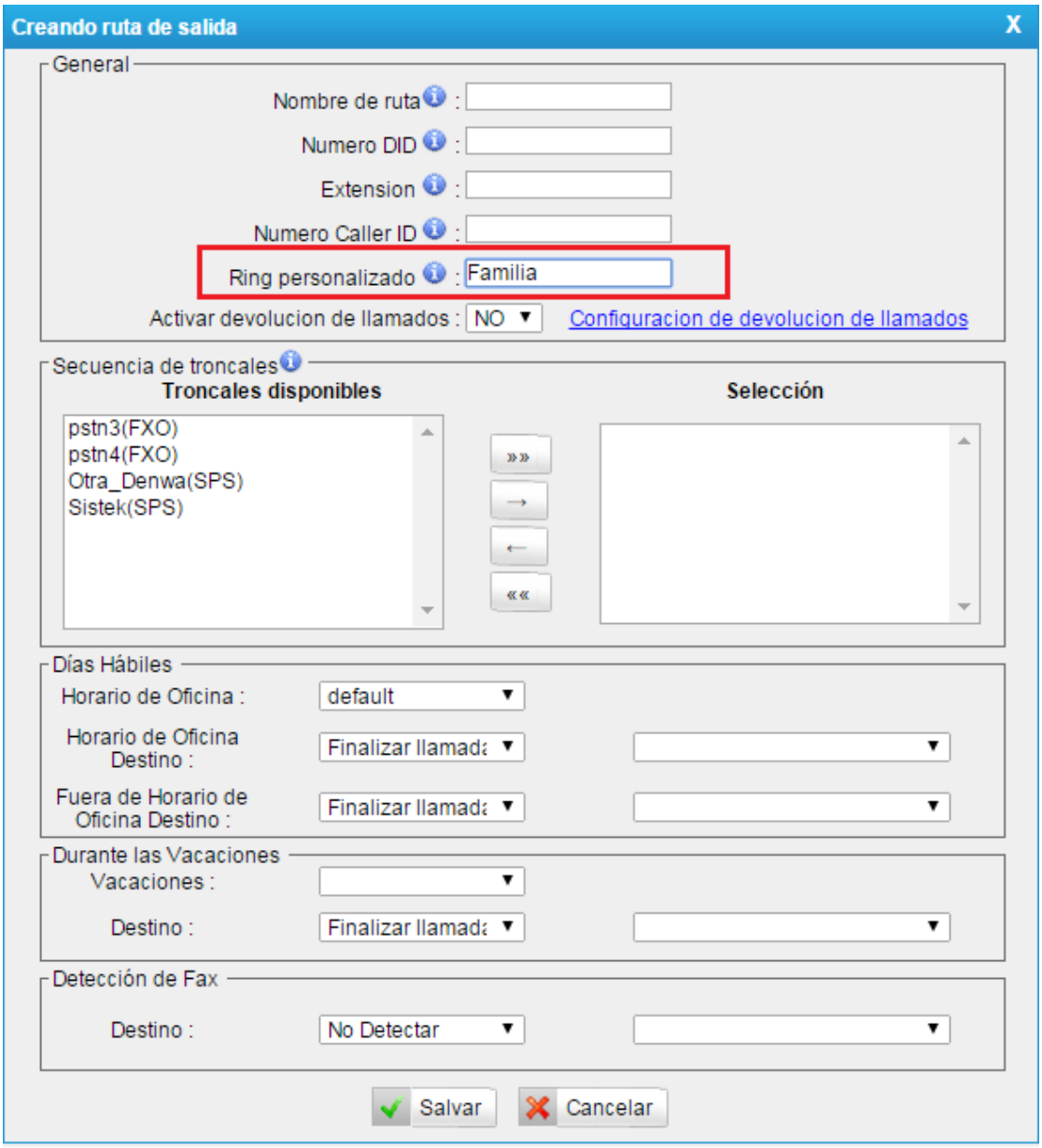


Figura E-2

Paso 3. Final.

APPENDIX F Cómo utiliza DID

Marcación interna directa (DID), también llamado directo dial-in (DDI) en Europa y Oceanía, es una función ofrecida por las compañías telefónicas para usar con sistemas de intercambio (PBX) rama privada de sus clientes. En servicio DID la compañía telefónica proporciona una o más líneas troncales al cliente para la conexión con PBX del cliente y asigna un rango de números de teléfono a esta línea (o grupo de líneas) y reenvían todas las llamadas a esos números a través del troncal.

UNI-K soporta DID, puede configurar DID en ruta entrante. Configuraciones relacionadas: **Número DID, Extensión, Destino.**

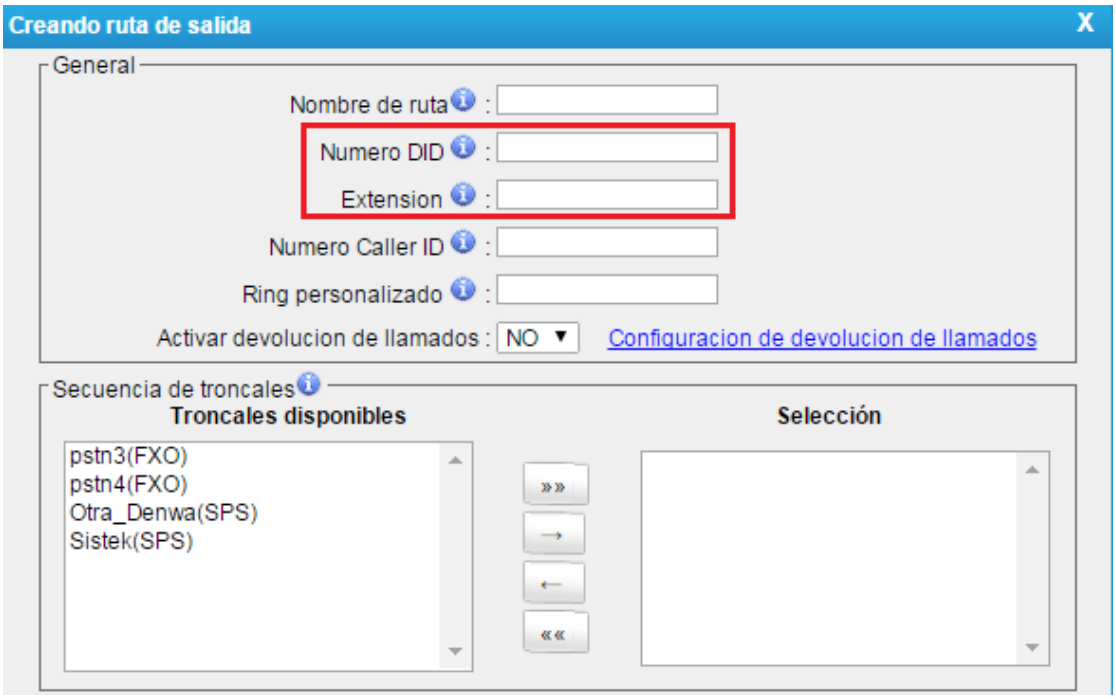


Figura F-1

·Número DID

Define el número DID esperado si este troncal pase DID en las llamadas entrantes. Deje este campo en blanco para que coincida con las llamadas con unas o sin DID información. Solo proveedor de servicio, E1 troncales, troncales BRI o troncales SIP necesitan ser configurados con esta configuración.

También puede utilizar la coincidencia de patrones para que coincida con un rango de números. Los patrones siguientes pueden ser utilizarse:

X: Algún dígito desde 0-9

Z: Algún dígito desde 1-9

N: Algún dígito desde 2-9
[12345-9]: Algún dígito en ménsulas (en este ejemplo, 1, 2, 3, 4, 5, 6, 7, 8, 9)
El "**.**" El carácter coincidirá con todos los dígitos restantes. Por ejemplo, "9011." coincidirá algún número telefónico que empiece con "9011", incluyendo "9011" .
El "**!**" Coincidirá con ninguno dígitos restantes, y hace que el proceso de correspondencia para completar lo antes que se pueda determinar que no hay otros partidos son posibles.

·Extensión
Define la extensión para el número DID, este campo solo disponible cuando utiliza troncal E1 para este router entrante. Puede solo ingresar número y "-" en éste campo, y el formato puede ser xxx o xxx-xxx. El recuento del número debe ser único o igual a la cuenta del número DID.

·Destinación
Si no puede configura la extensión, puede configura el destino de la llamada aquí.

Ejemplo 1:
Paso1: Configura el número DID (5503XXX en este ejemplo).
Paso 2: Puede seleccione el destino (IVR en este ejemplo).

La configuración de este ejemplo significa cuando la llamada entrante con número DID 5503XXX (número de 7 dígitos empiece con 5503) irá al destino IVR.

Si seleccione el destino, por favor deje la Extensión desde en blanco.

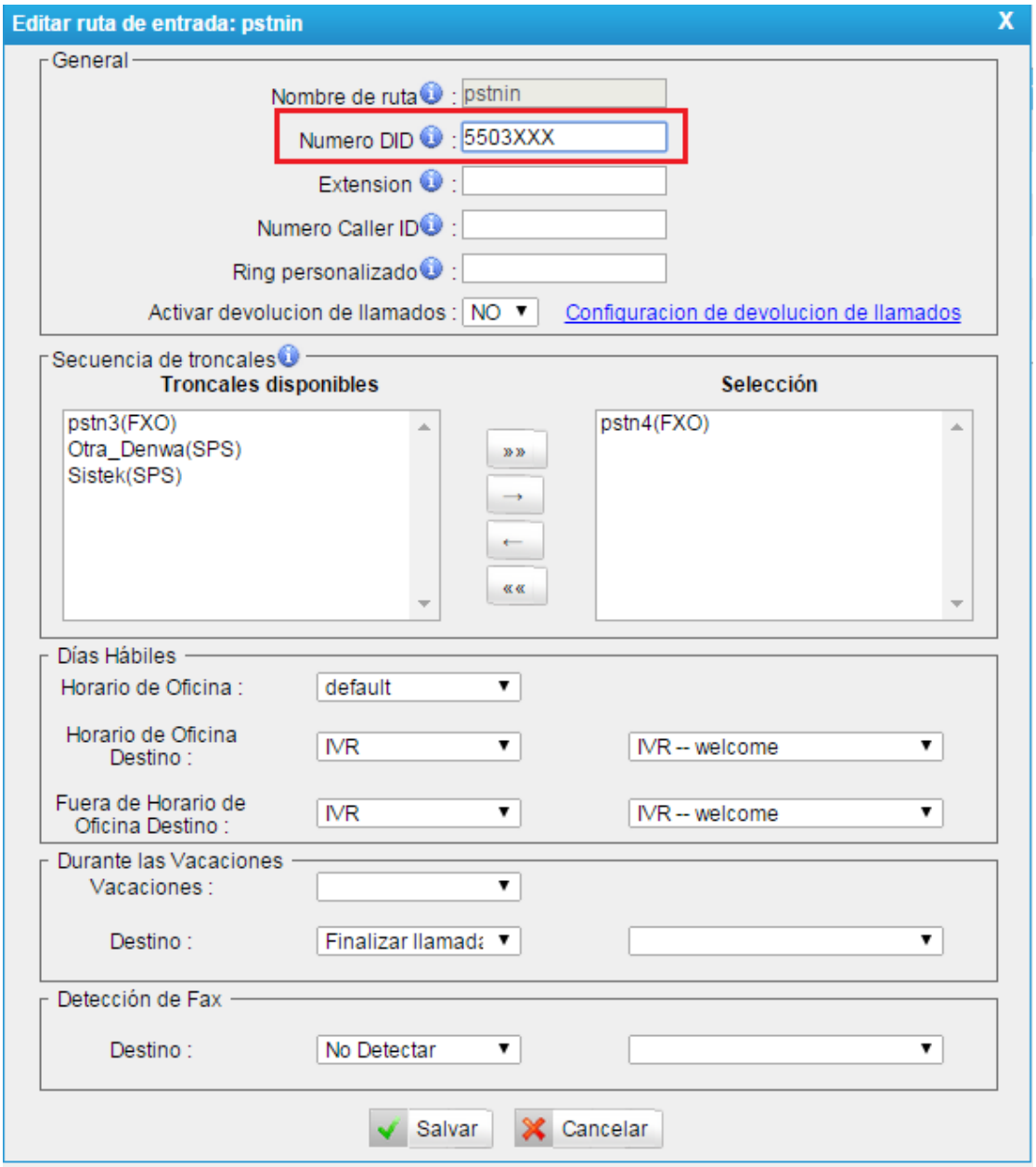


Figura F-2

Ejemplo 2:
Paso1: Configura el número DID (6001-6099 en este ejemplo).
Paso 2: Configura la Extensión (6001-6099 en este ejemplo).

La configuración de este ejemplo significa cuando la llamada entrante con DID número 6001 a 6099 se irá al destino 6001 a 6099 (número 6001 a extensión 6001, número 6002 a extensión 6002).

El destino establece abajo será desactivado si configura la Extensión.

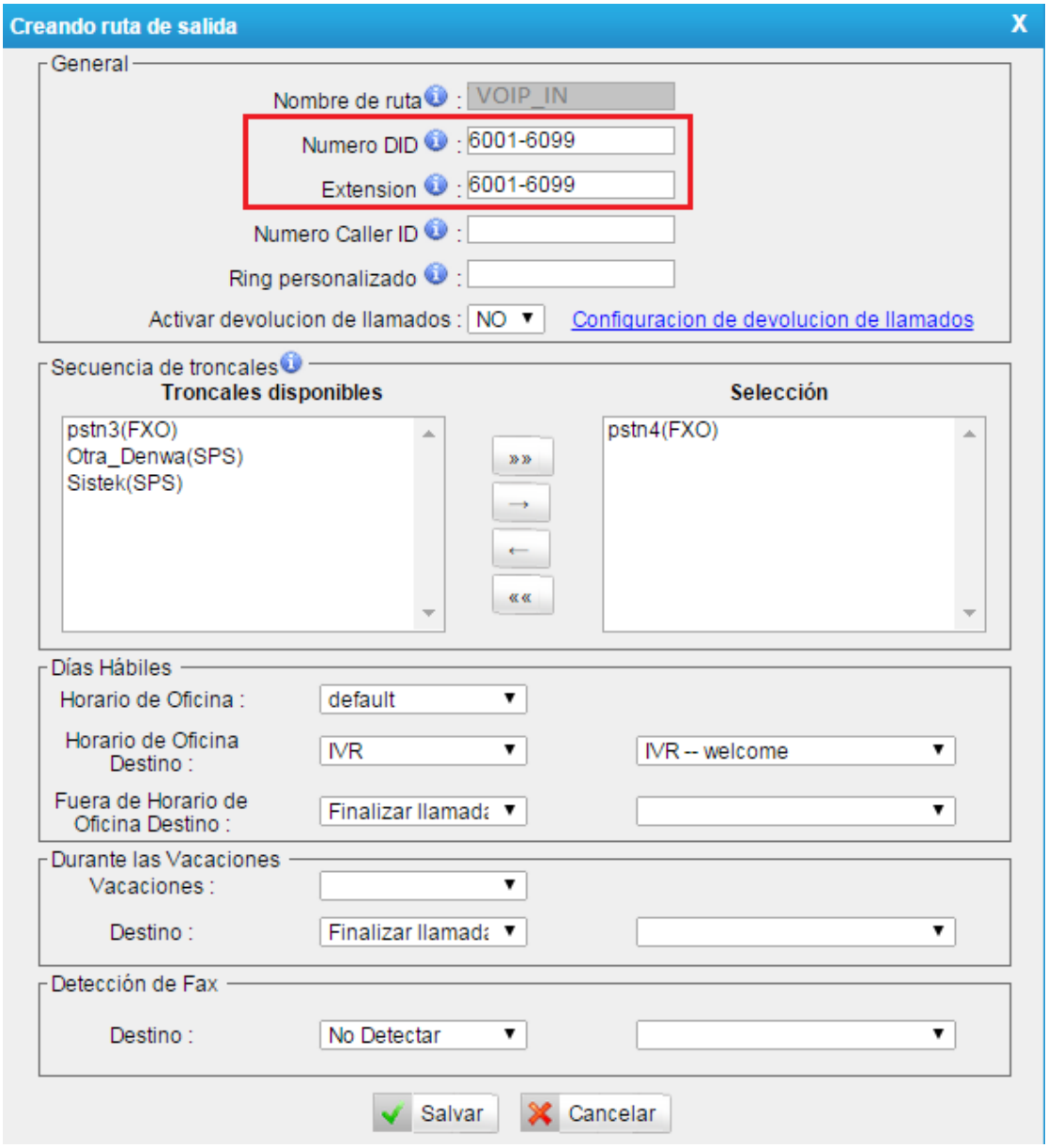

Creando ruta de salida
X
General
Nombre de ruta : VOIP_IN
Numero DID : 6001-6099
Extension : 6001-6099
Numero Caller ID :
Ring personalizado :
Activar devolucion de llamados : NO
Configuracion de devolucion de llamados
Secuencia de troncales
Troncales disponibles
Selección
pstn3(FXO)
Otra_Denwa(SPS)
Sistek(SPS)
pstn4(FXO)
Días Hábiles
Horario de Oficina : default
Horario de Oficina Destino : IVR
IVR -- welcome
Fuera de Horario de Oficina Destino : Finalizar llamad
Durante las Vacaciones
Vacaciones :
Destino : Finalizar llamad
Detección de Fax
Destino : No Detectar
Salvar
Cancelar

Figura F-3

APPENDIX G ¿Cómo utiliza Tecla BLF a Seleccionar Línea PSTN?

UNI-K le permite a seleccionar Línea PSTN especificada a hacer llamada saliente mediante el presionado la tecla BLF en Teléfono IP.

Sigue los pasos a hacer la configuración con su teléfono Yealink.

1. Queremos seleccionar pstn1 o pstn2 a hacer llamada.

Figura G-1

2. Configura el teléfono IP:

Figura G-2

Prueba
Cuando presione tecla DSS 1/2, el teléfono conectará a línea pstn1/pstn2. Si pstn1/pstn2 es no ocupada, escuchará el tono del marcad. Puede marcar el número que quiere y utiliza esta línea a llamarse luego.

APPENDIX H Guía de Configuración de Seguridad de UNI-K

VoIP ataques, aunque no es una ocurrencia diaria, pero existe. Durante el uso de VoIP, seguridad del sistema es sin duda uno de los temas que nos importan más. Pero con la configuración apropiada y algunos hábitos de seguridad básica, podemos mejorar la seguridad del sistema telefónico. Además, la función potente firewall incorporado en UNI-K es adecuada para permitir que el sistema funcione de manera segura y estable.

Esta guía presenta el nivel mayor de defensa en UNI-K, y le recomendamos que configure firewall y otras opciones de seguridad según esta guía, para evitar el fraude de ataque y la pérdida de llamadas o fallo del sistema.

Notas:
1. En esta guía, las opciones de configuración marcaron con "*" sólo existe en X.18.XX.XX y sobre las versiones.
2. Le recomendamos a actualizar el firmware a la última versión para propósito de seguridad.
3. No asigna algún puerto a UNI-K en router Si no es necesario.
4. Recomendamos a limitar el crédito de VoIP troncales para llamadas internacionales.

Centro de Seguridad*

Centro de seguridad es una nueva característica desde x.18.0.xx, podremos tener una visión general de configuración básica como firewall, servicio de seguridad y guardia el puerto.

Clic "Sistema→ Preferencias de Sistema→Centro de Seguridad" a obtener los detalles. Puede hacer clic en el botón a configurar estos uno por uno. Puede seguir los pasos en este manual a configurar y obtener el resultado en esta página.

1. Puerto:

Esta página se muestra el puerto SIP y HTTP, podemos hacer clic en "Configuración" a cambiarlo.
Es recomendable que se debería cambiar el puerto predeterminado.

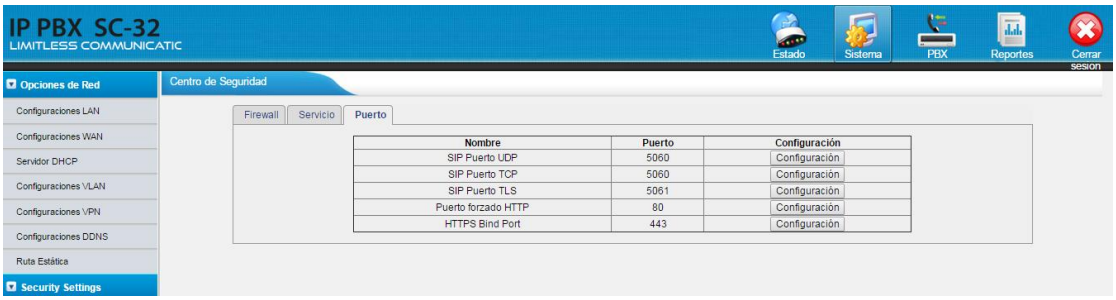


Figura H-0-1

2. Service:

Esta página muestra el servicio general como AMI, SSH y TFTP, recomendamos a desactivarlo si no es necesario.

Nota: TFTP se utiliza para el aprovisionamiento de teléfono, está habilitada de forma predeterminada, puede desactivarlo después de todos los teléfonos están bien configurados.

Figura H-0-2

3. Firewall:

En esta página, la información básica de reglas de firewall son mostradas. Recomendamos a configurar paso a paso siguiendo parte 2 de este manual.

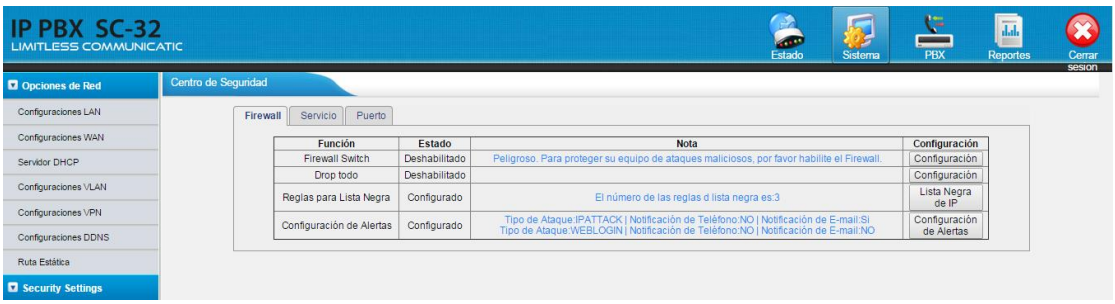


Figura H-0-3

1. Puertos y realce de contraseña

Los puertos y la contraseña son más importantes para la seguridad; se recomienda cambiar el valor por defecto al algún propio.

1.1 Web GUI (HTTP)

1.1.1 Cambiar el puerto de enlace HTTP predeterminado.

PBX→Configuraciones Básicas→ Preferencias Generales→HTTP Puerto Unido

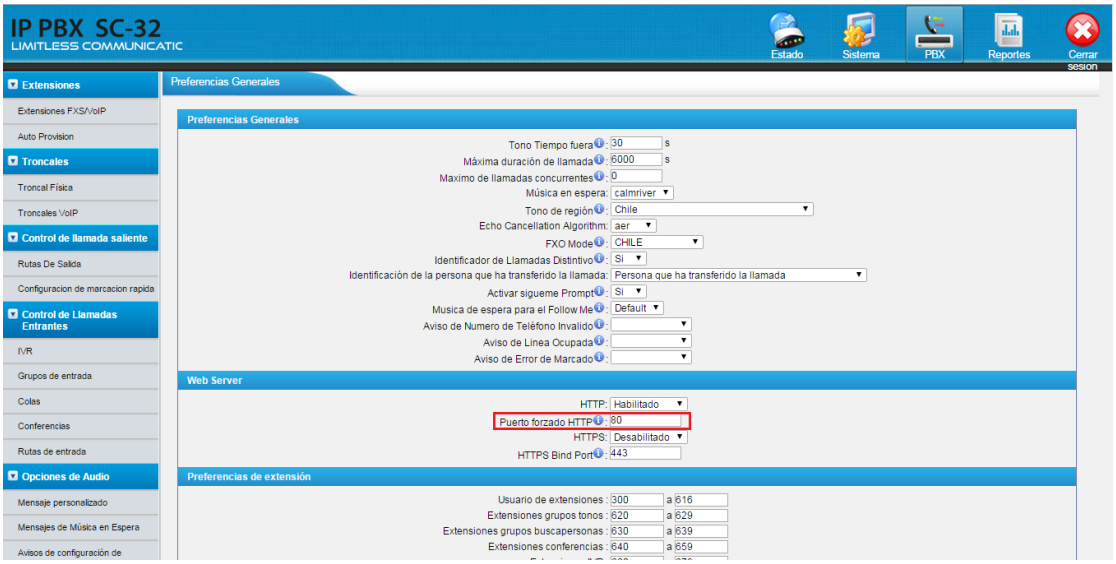


Figura H-1-1

Podemos cambiarlo al algún otro como 8080 por ejemplo.

1.1.2 Cambia la contraseña predeterminada.

Sistema→ Preferencias del Sistema→Cambiar Contraseña

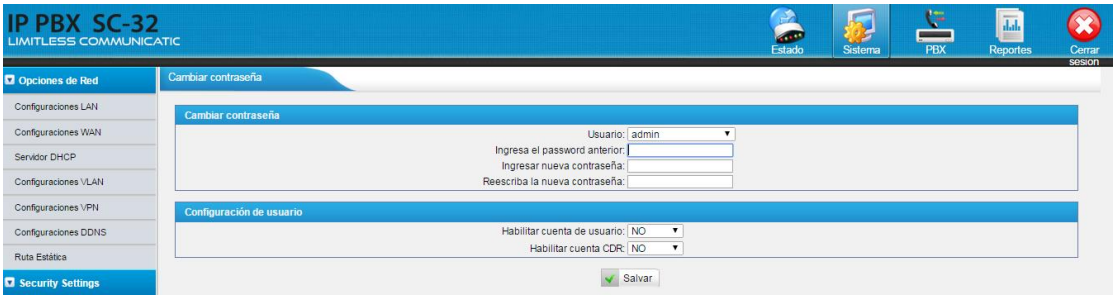


Figura H-1-2

Una contraseña segura debe configurarse aquí para todas las cuentas. Especialmente cuentas “admin” y “user”.

1.2 Extensión

Los hackers siempre están enviando paquetes a PBX para registrar la extensión antes de marcar hacia fuera. La seguridad de extensión es muy importante para los usuarios.

1.2.1 Cambia el Puerto SIP Predeterminado

PBX→Configuraciones Básicas→Configuraciones de SIP→General→UDP Puerto

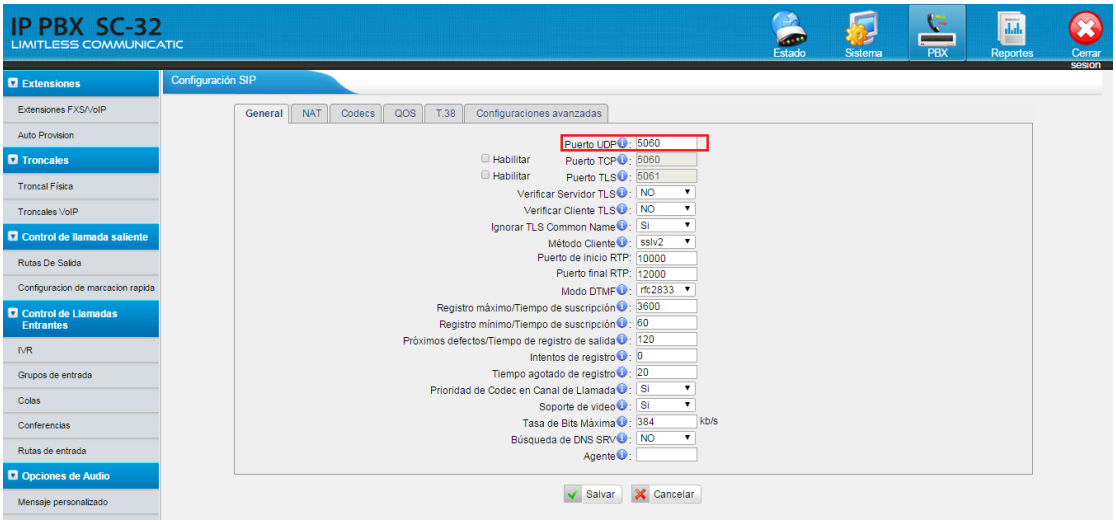


Figura H-1-3

Se recomienda cambiar esto a otro puerto disponible, por ejemplo: 5080.

1.2.2 Cambia la contraseña predeterminada.

La contraseña de las extensiones es "pincode + número de extensión". Se recomienda una contraseña con números y letras superiores e inferiores. Por ejemplo: AjK5Up1G.

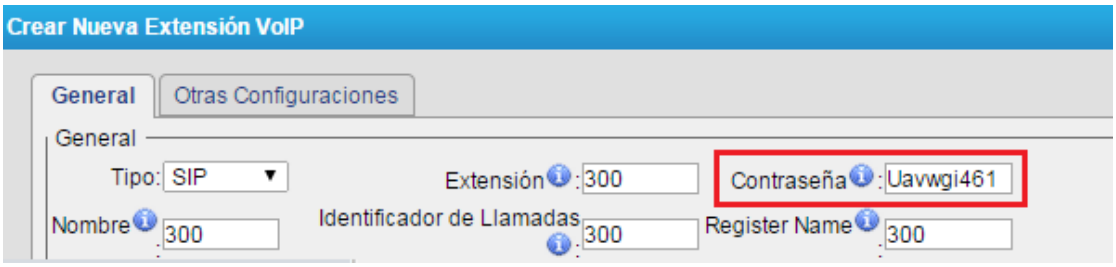


Figura H-1-4

Nota: Una contraseña segura es una necesidad para las extensiones remotas.

1.2.3. Restricción de IP para las extensiones

Puede encontrar esta configuración en PBX→Extensiones→FXS/VoIP Extensiones→ VoIP Extensiones→General→Contraseña
Cuando está configurada, solo IP permitida puede registrar esta extensión. Todas las solicitudes de registro serán negadas.

El formato es "dirección IP/Subnet mask", por ejemplo 192.168.5.136/255.255.255.255. En esta forma, sólo 192.168.5.136 puede registrar esta extensión 6010.

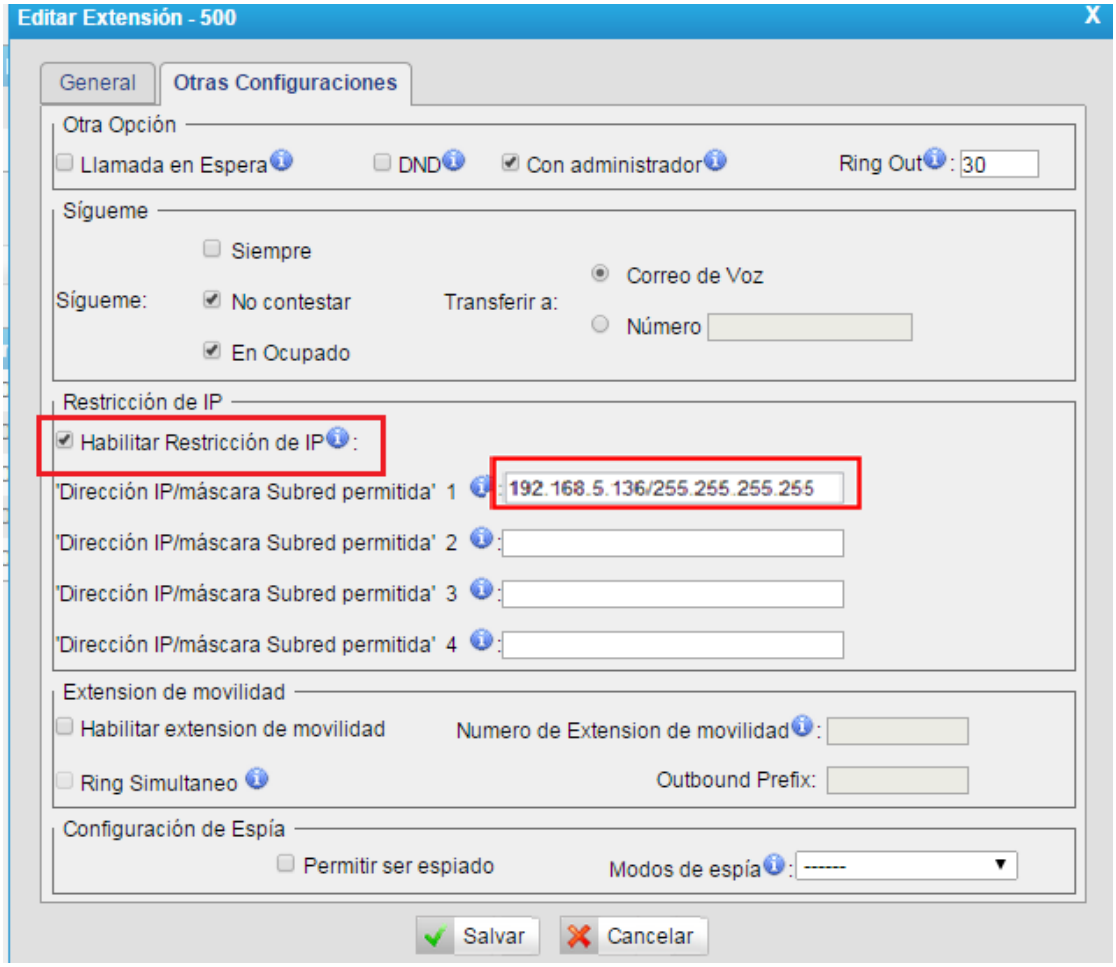


Figura H-1-5

Nota: Si es por extensión remota, una dirección IP pública estática es necesaria para la entrada en su lugar.

1.2.3 Configuración de Seguridad para las Extensiones Remotas

PBX→Extensiones→FXS/VoIP Extensiones→ VoIP Extensiones→General habilita "NAT" y "Registra remotamente" como en la foto se muestra a continuación.

Figura H-1-6

Notas:

1. Si el registro externo no se requiere, por favor lo desactiva.
2. Si las extensiones registran a UNI-K vía puerto WAN, por favor, sólo permiten "registra remotamente".

1.2.4 TLS registro (Opcional)

Introducción

Seguridad de capa de transporte (TLS) y su predecesor, Secure Sockets Layer (SSL), son protocolos criptográficos que proporcionan seguridad de las comunicaciones mediante Internet. Usan criptografía asimétrica para la autentificación de intercambio de claves, cifrado simétrico para garantizar la confidencialidad y códigos de autenticación de mensaje para la integridad del mensaje. Varias versiones de los protocolos son de uso generalizado en aplicaciones tales como navegación web, correo electrónico, fax de Internet, mensajería instantánea y voz sobre IP (VoIP).

TLS es soportado en UNI-K para seguridad de registro de SIP; también puede registrar troncales SIP para los proveedores de VoIP mediante TLS. Tenemos que cargar el certificado en UNI-K y los teléfonos IP juntos para la autorización.

Los hackers envían la solicitud de registro a PBX para registro vía UDP por lo general, si TLS está habilitada en UNI-K, hacker no puede registrar la extensión sin el CA, directamente se rechazará la solicitud de registro.

Consulta a **Appendix I** a obtener los detalles de pasos de como utiliza TLS en UNI-K.

Nota: TLS está desactivado en UNI-K por defecto; Tenemos que activarlo en la página "Configuración de SIP" por adelantado antes de usarlo.

2. Configuración de Firewall

Nota: Haga copias de seguridad de las configuraciones de copia de seguridad y restaurar la página antes de adelante. En el caso que es bloquea el dispositivo, puede restablecer a valores de fábrica y restaurar las configuraciones anteriores. Las reglas del ejemplo siguientes trabajar con con UNI-K firmware versión 2.15.xx.xx o versiones superiores.

La lógica básica para configurar firewall es "Permiten todas las direcciones IP confiadas y luego activar "Dejar todo"".

Paso1. Habilita firewall en la página de firewall de UNI-K.

Sistema→Firewall Configuraciones→ Reglas de Firewall →Configuraciones Generales

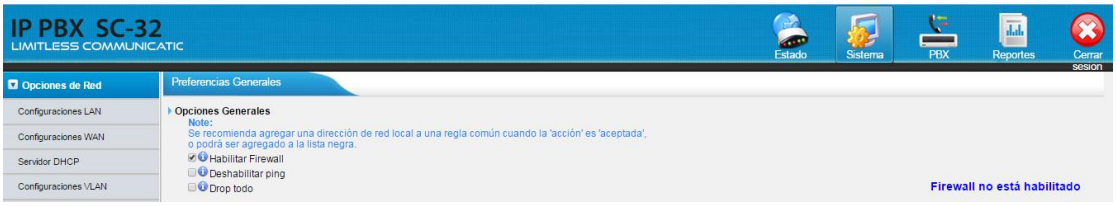


Figura H-2-1

Paso2. Añaden reglas comunes a aceptar el acceso de la red local.

Crear una regla común para permitir todas las direcciones IP de los teléfonos locales tengan acceso al servidor UNI-K. Por ejemplo, el rango de IP local es 192.168.5.1-192.168.5.254, la configuración podría ser como a continuación:

Nombre: LocalNetwork
Protocolo: BOTH
Puerto: 1:65535
IP: 192.168.5.0/255.255.255.0, el formato debe ser "IP/net mask"
Acción: Acept.

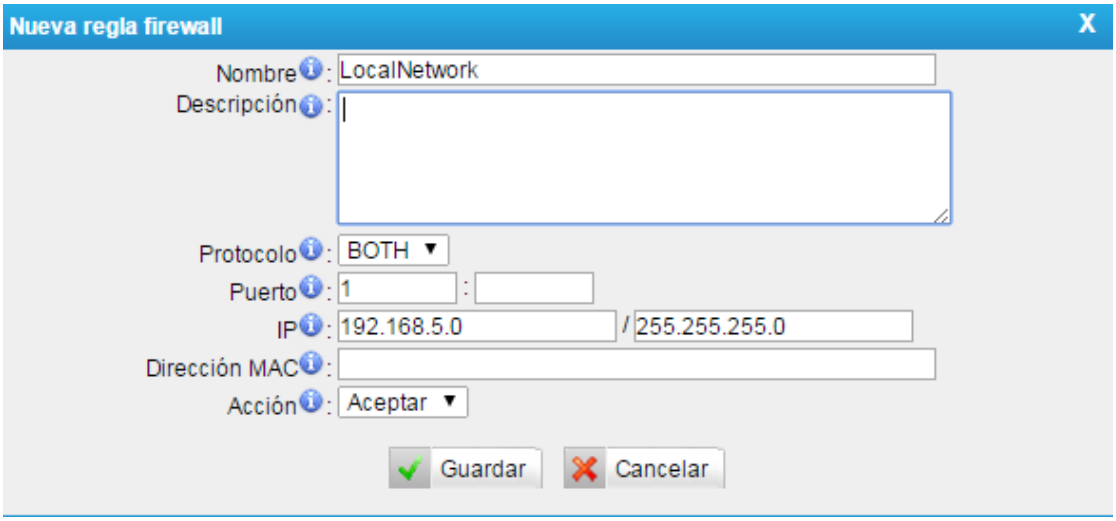


Figura H-2-2

Paso3. Agregan las reglas comunes a permitir administradores, extensiones o dispositivos remotos

Por ejemplo IP pública es 110.30.25.152; podemos permitir todos los puertos para esta IP confiada.

Nombre: Remoto
Protocolo: BOTH
Puerto: 1:65535
IP: 110.30.25.152/255.255.255.255
Acción: Acept.

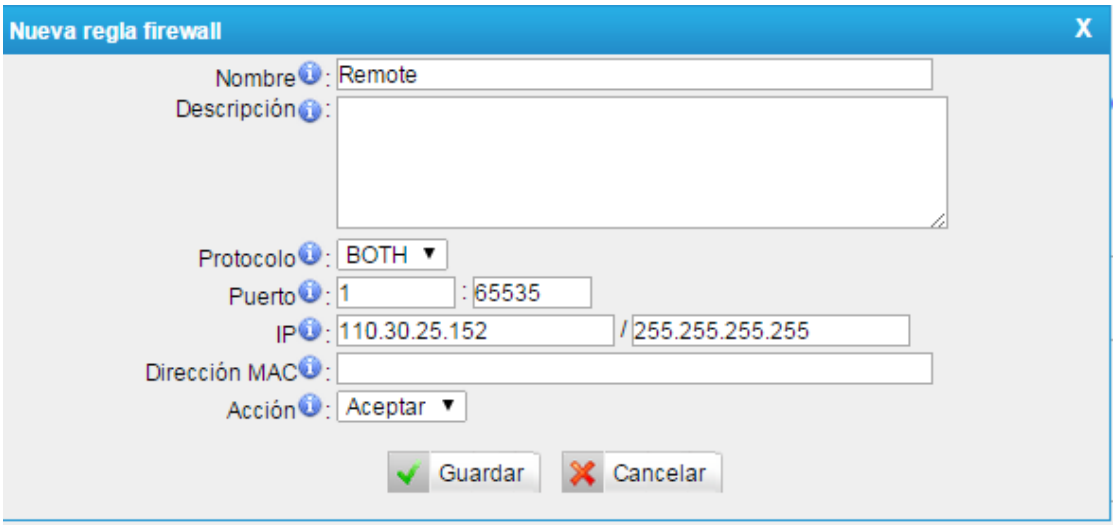


Figura H-2-3

Nota: Rango de IP pública estática debe configurarse aquí, si es IP address dinámico que no pertenecen a un rango, no hay necesidad de configurarlo, pero "The Drop All" en el próximo paso no debe estar marcada. Las Reglas de lista negra de IP ayudará a proteger UNI-K. Recomendamos a obtener IP pública estática para propósito de seguridad.

Paso4. Agregan las reglas comunes a aceptar rango de IP pública estática del proveedor VoIP.

Los puertos utilizados para contactar proveedor SIP es 5060 y 10000-12000 por defecto, si había cambiado el rango de puerto, puede introducirlo aquí por sí mismo.

Por ejemplo, la dirección IP es 110.111.132.6, las configuraciones deberán ser dos partes, una es para 5060, y la segunda es para puerto RTP: 10000-12000.

Permite registro del puerto: 5060.

Nombre: SIP
Protocolo: UDP
Puerto: 5060:5060
IP: 110.111.132.6/255.255.255.255
Acción: Acept.

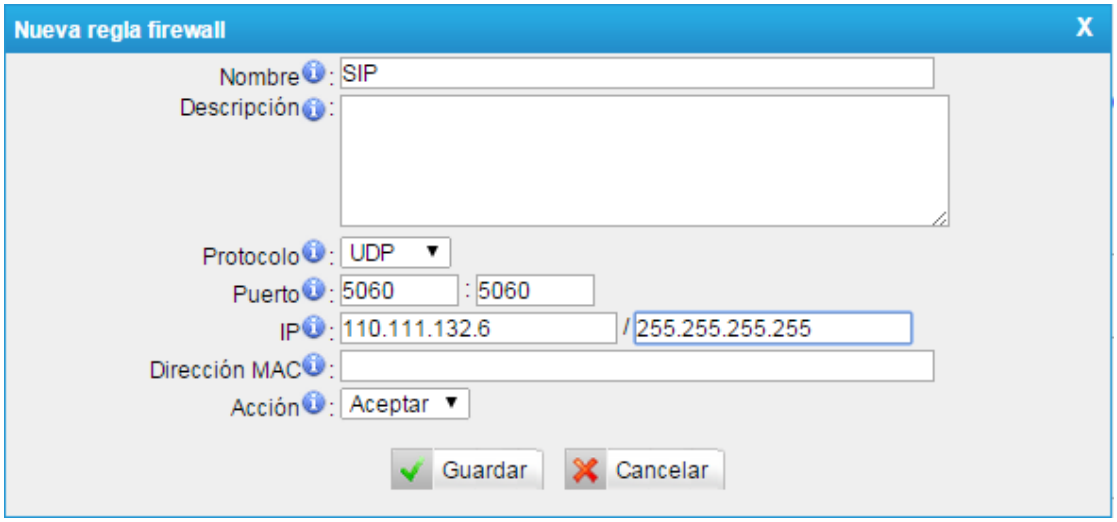


Figura H-2-4

Rango de puerto RTP permitido:

Nombre: RTP
Protocolo: UDP
Puerto: 10000:12000
IP: 110.111.132.6/255.255.255.255
Acción: Acept.

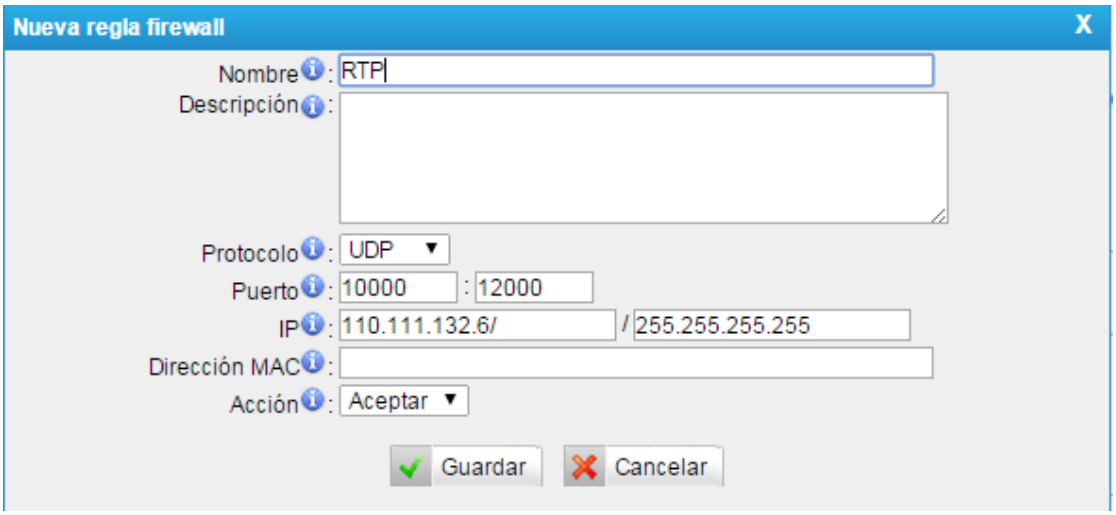


Figura H-2-5

Nota: Si el servidor de medios del proveedor SIP es dinámico, y no podemos cobrar el rango de IP. Podemos permitir que el rango de RTP para las direcciones IP como esto:

Nombre: RTP_ALL

Protocolo: UDP
Puerto: 10000:12000
IP: 0.0.0.0/0.0.0.0
Acción: Acept.

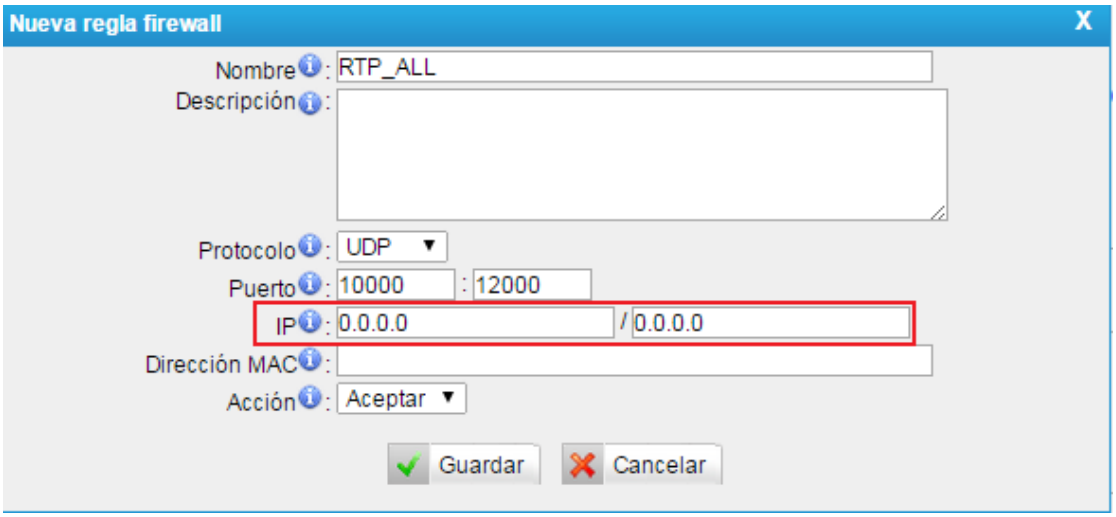


Figura H-2-6

En este caso, UNI-K puede deshacerse de ida volumen número.

Paso5. Bloquea la conexión de la web de la otra dirección IP que no se agregan a la lista de aceptada.

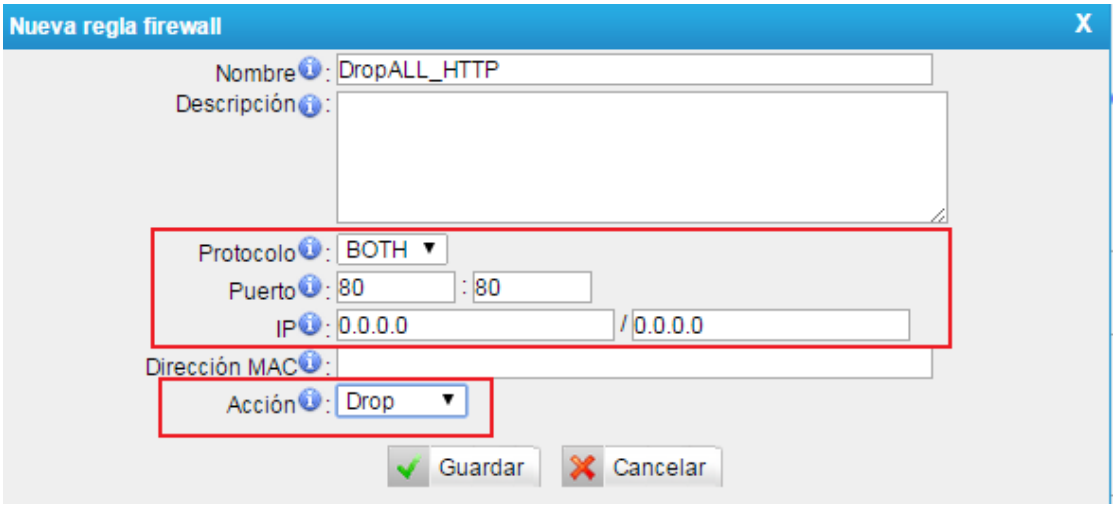


Figura H-2-7

Nota: Muchos ataques son causados por el acceso al web, se recomienda altamente para soltar la conexión no es de confianza vía interfaz web.

Paso 6: Agregan las reglas comunes a aceptar rango de IP pública estática del servidor NTP, SMTP, y POP.

Recomendamos a abrir todos los puertos para servidor NTP, SMTP y POP en firewall de UNI-K y la dirección IP debe ser una estática o pertenece a un rango. Si es Dyndns, no hay necesidad de configurar esta regla, pero debe mantenerse la lista negra IP, y "Dejar todo" no debe estar marcado.

Por ejemplo, el servidor SMTP es 110.30.1.123.

Nombre: Allow_SMTP
Protocolo: BOTH
Puerto: 1:65535
IP: 110.30.1.123/255.255.255.255
Acción: Acept.

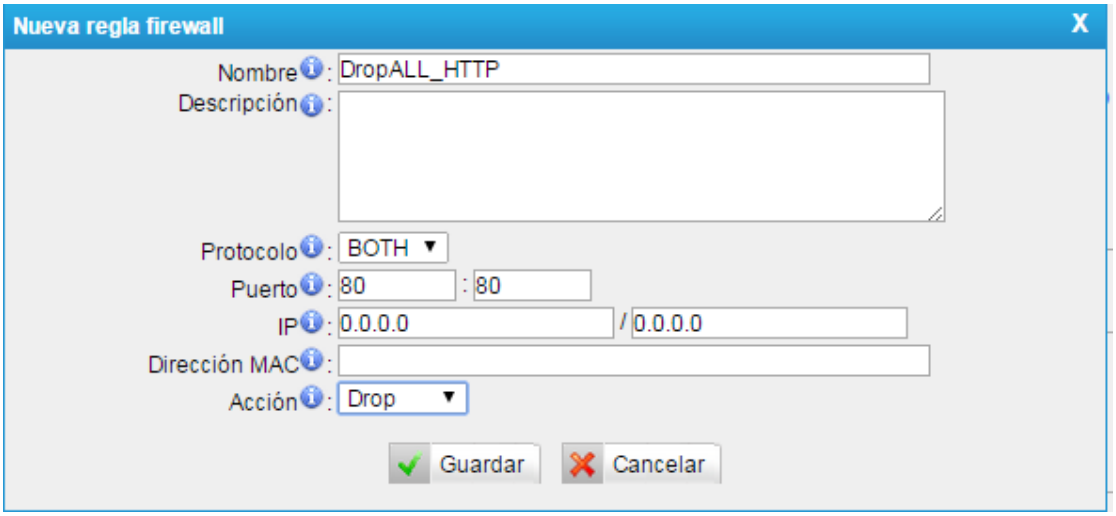


Figura H-2-7

En cuanto a la regla del servidor NTP y POP, se puede crear uno por uno.

Paso 6. Configura reglas automáticas de lista negra

Reglas automáticas de lista negra: el servidor añadiría la dirección IP a la lista negra automáticamente si el número de los paquetes que envía excede la regla que ha configurada.

Nota: Hay 3 reglas están configuradas por UNI-K por defecto.

1) Añade dos reglas automáticas de lista negra para puerto: 5060.

Regla No.1:

Puerto: 5060
Protocolo: UDP
Paquetes IP: 120
Tiempo intervalo: 60 segundos

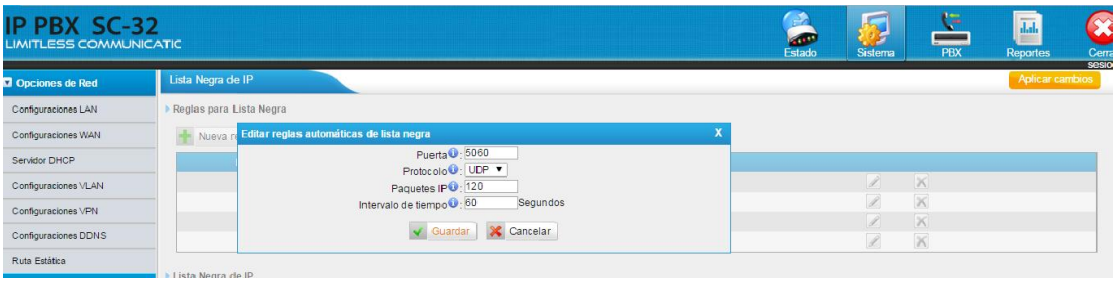


Figura H-2-8

Regla No.2:

Puerto: 5060
Protocolo: UDP
Paquetes IP: 40
Tiempo intervalo: 2 segundos

Figura H-2-9

2) Añade una regla automática de lista negra para puerto:8022

Regla No.3

Puerto: 8022
Protocolo: TCP
Paquetes IP: 5
Tiempo intervalo: 60 segundos

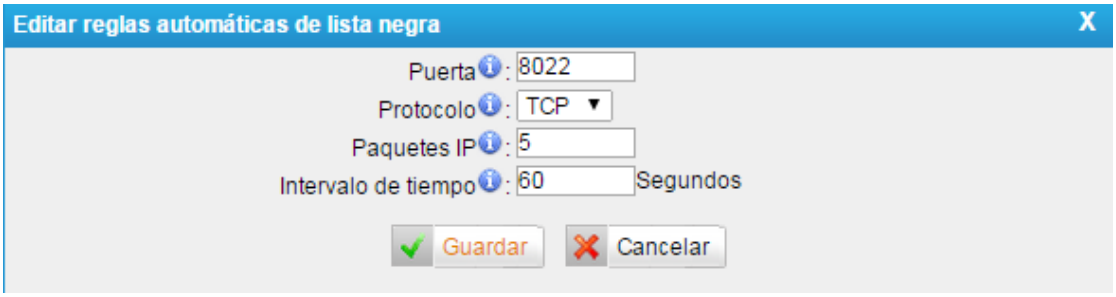


Figura H-2-10

Paso 7. Habilitar "Caen todos" (si esta función está activada, todos los paquetes y conexión que no coinciden con las reglas que se caerán.)

Advertencia: Antes de activar esta función, por favor crea una regla para aceptar el acceso a la red local, si no el servidor no puede tener acceso.

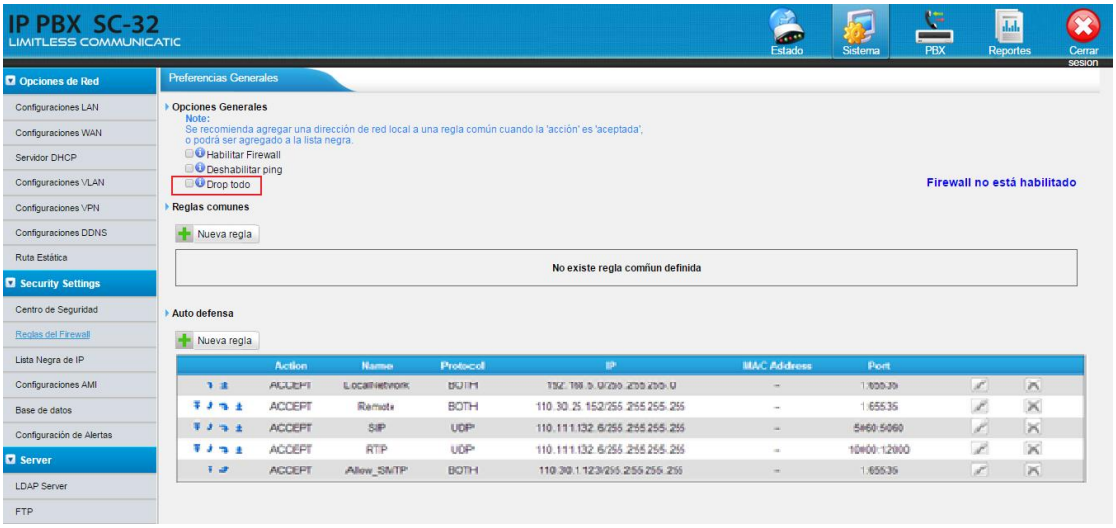


Figura H-2-11

Notas:

1. Después de habilitar "Caer todo", las reglas de la auto defensa y lista negra de IP no tendrá efecto. Significa excepto el IPs y paquetes que están definidos en las reglas aceptadas, la otra conexión o paquetes caerán.
2. Si no está activado "caer todos", por favor, no retire las reglas de la lista negra IP en caso el agujero de seguridad del sistema existentes.

Paso 8. La configuración de configuraciones firewall es completada. Vea los ejemplos de abajo.

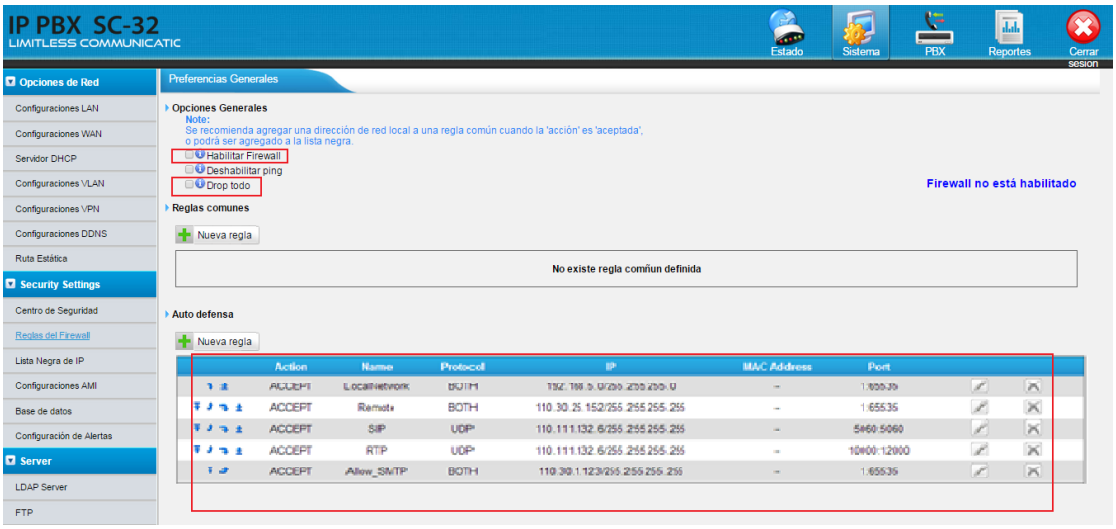


Figura H-2-12

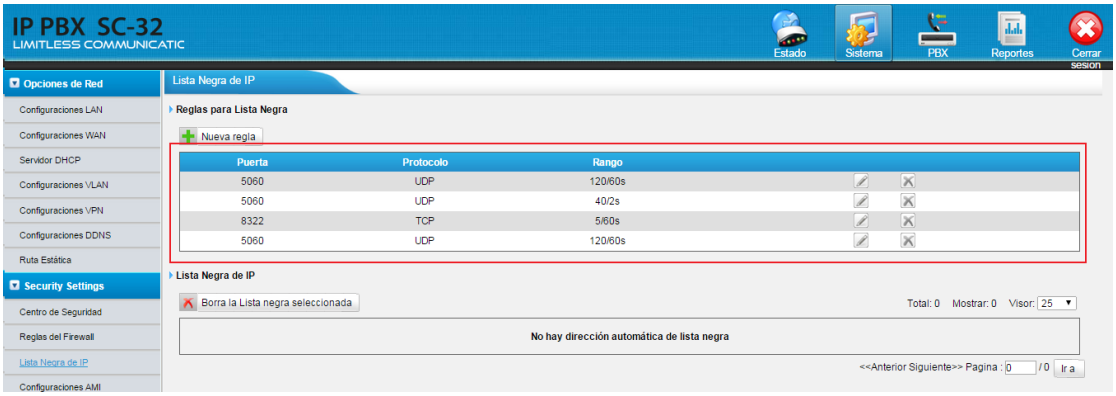


Figura H-2-13

3. Seguridad del servicio

3.1 Desactiva Llamadas de Guest

3.2 Desactiva Llamadas de Guest

PBX→Configuraciones Básicas→Configuraciones de SIP→Configuraciones Avanzadas→Permite Guest

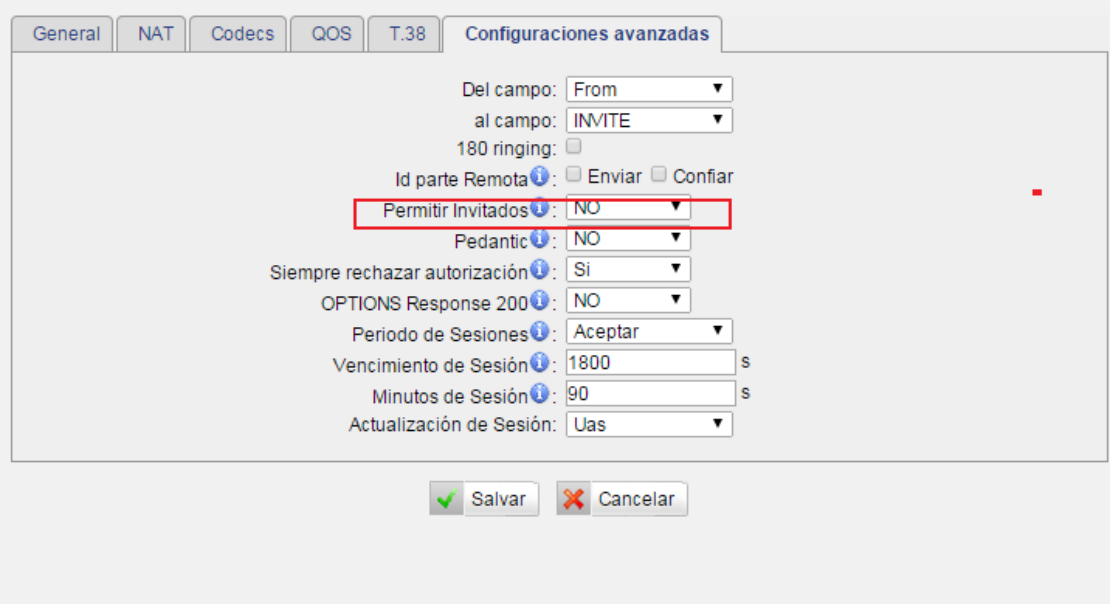


Figura H-3-1

Nota: Permite Guest está deshabilitado por defecto; por favor, mantenga en "No" para uso general.

3.3 Configuraciones de AMI*

La Interfaz de Asterisk Gestión (AMI) permite que un programa del cliente para conectarse a una instancia de Asterisk y orden de edición o leer eventos sobre una corriente de TCP/IP. Los integradores encuentran está particularmente útil cuando se trata de rastrear el estado de un cliente de telefonía dentro de Asterisk y dirigir a ese cliente basado en reglas personalizadas (y posiblemente dinámicas).
Para más información, puede consultar a esta página:
http://www.voip-info.org/wiki/view/Asterisk+manager+API

Nota: esta funcionalidad es desactivada por defecto; no hay necesidad de activarla para el uso general. Si es desactivada, por favor cambia la cuenta y configura la restricción de IP.

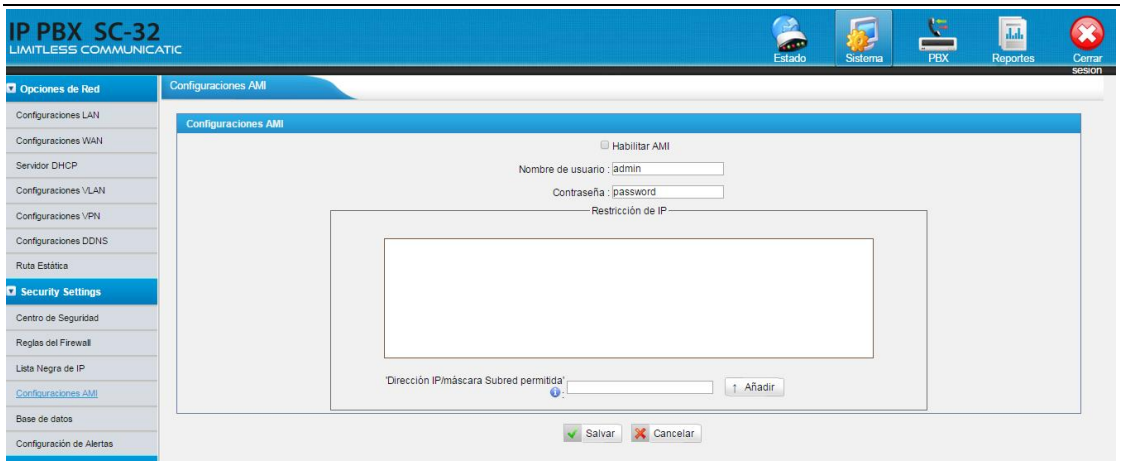


Figura H-3-6

Para administrar las cuentas para acceder a AMI, podemos configurarlo en página AMI directamente. Haga clic en Sistema→Preferencias de Sistema→Configuraciones de AMI.

Por ejemplo, la cuenta AMI que necesite es:
Nombre de Usuario: Developer
Contraseña: Developer
Sólo la dirección IP que permitida a iniciar sección es 192.168.1.71.

Podemos configurarla como este:

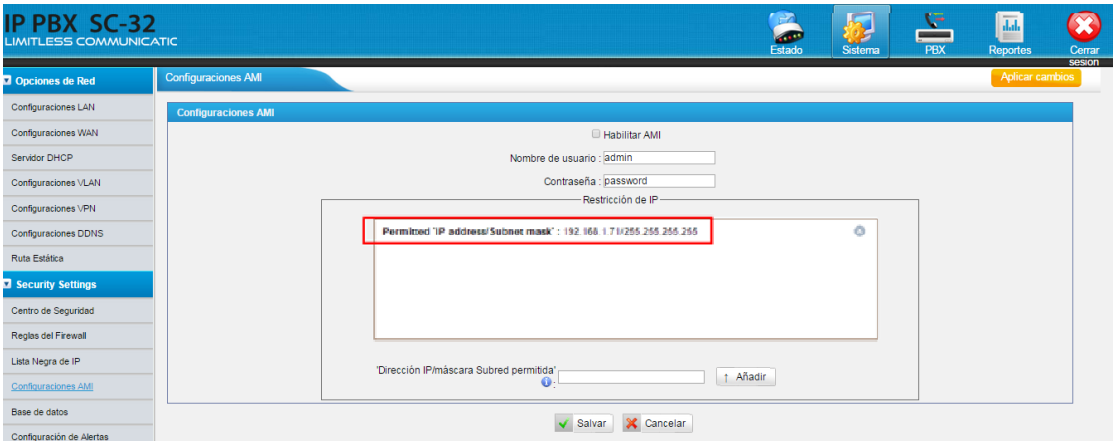


Figura H-3-7

Guarda la y aplica el cambio.

3.4 TFTP*

UNI-K puede trabajarse como un servidor TFTP cuando utilizando "teléfono aprovisionamiento", y esta funcionalidad está desactivado por defecto. Si todos los teléfonos son provisionados bien, puede desactivar este acceso a proteger los archivos de configuración de UNI-K.

Clic "Sistema→Centro de Seguridad→Servicio" a desactivarla directamente.

Figura H-3-9

3.5 Concesión de Database*

UNI-K ha integrado MySQL desde x.18.0.xx, que proporciona la conveniencia para los usuarios a gestionar CDR y el registro de grabación. Para proteger el acceso de database, tenemos que configurar el nombre de usuario y contraseña por separado antes de iniciar sesión.

No hay ninguna cuenta configurada por defecto, si quiere conectar la database usando software de tercero, es necesario a establecer esta primera.

Por ejemplo, nombre de usuario: Harry, contraseña: Harry123

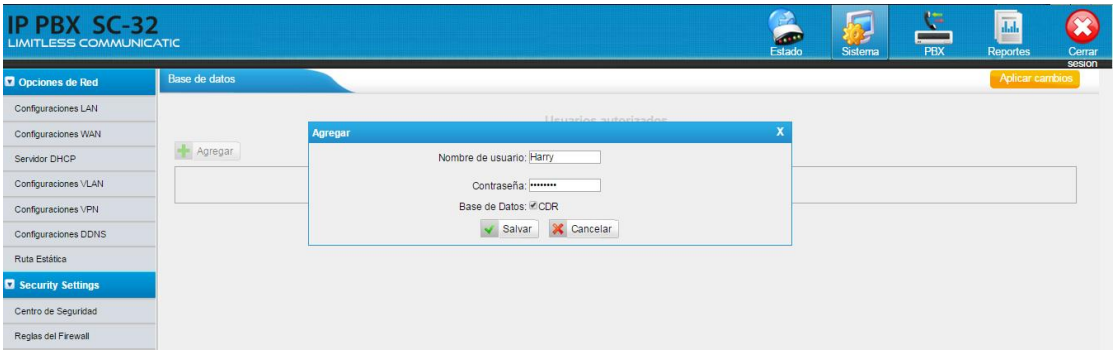


Figura H-3-10

Guarde y aplique el cambio.

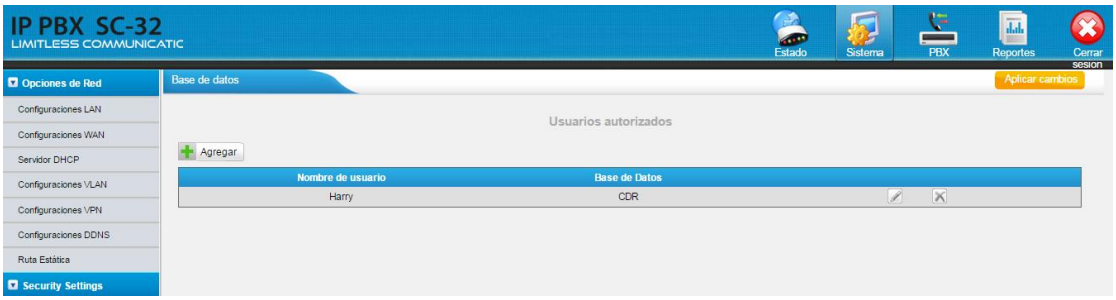


Figura H-3-11

Cuando se inicia el uso de otro software, podemos comprobar la CDR.

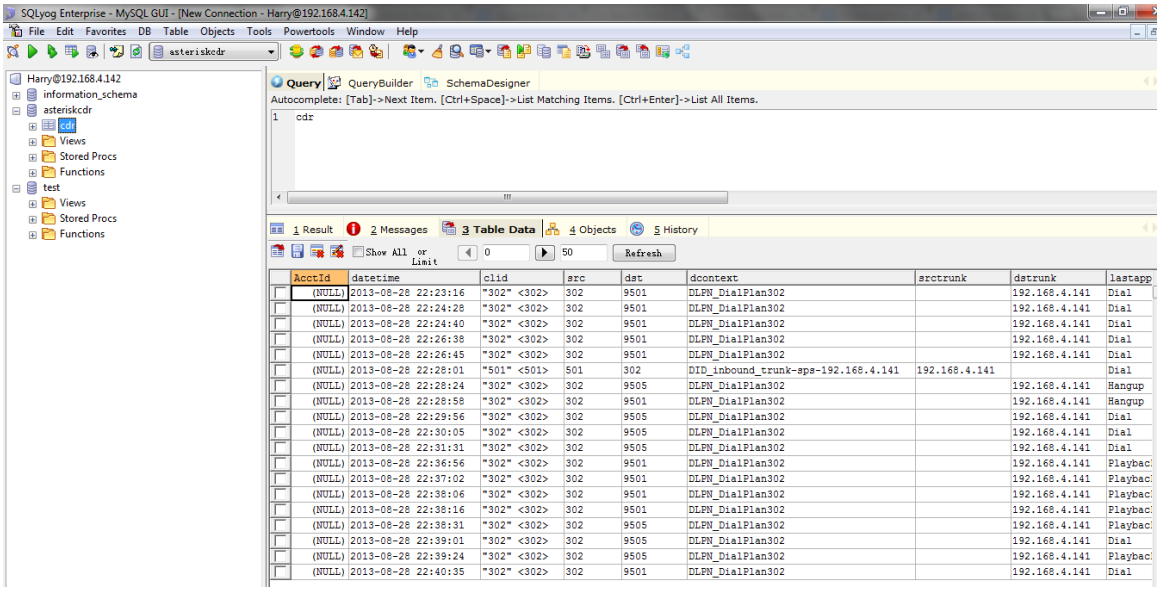

SQLyog Enterprise - MySQL GUI - [New Connection - Harry@192.168.4.142]
File Edit Favorites DB Table Objects Tools Powertools Window Help
Harry@192.168.4.142
information_schema
asteriskcdr
cdr
Views
Stored Procs
Functions
test
Views
Stored Procs
Functions
Query QueryBuilder SchemaDesigner
Autocomplete: [Tab]->Next Item. [Ctrl+Space]->List Matching Items. [Ctrl+Enter]->List All Items.
1 cdr
1 Result 2 Messages 3 Table Data 4 Objects 5 History
Refresh
AcctId datetime clid src dst dcontext srctrunk dstrunk lastapp
(NULL) 2013-08-28 22:23:16 "302" <302> 302 9501 DLPN_DialPlan302 192.168.4.141 Dial
(NULL) 2013-08-28 22:24:28 "302" <302> 302 9501 DLPN_DialPlan302 192.168.4.141 Dial
(NULL) 2013-08-28 22:24:40 "302" <302> 302 9501 DLPN_DialPlan302 192.168.4.141 Dial
(NULL) 2013-08-28 22:26:38 "302" <302> 302 9501 DLPN_DialPlan302 192.168.4.141 Dial
(NULL) 2013-08-28 22:26:45 "302" <302> 302 9501 DLPN_DialPlan302 192.168.4.141 Dial
(NULL) 2013-08-28 22:28:01 "501" <501> 501 302 DID_inbound_trunk-sps-192.168.4.141 192.168.4.141 Dial
(NULL) 2013-08-28 22:28:24 "302" <302> 302 9505 DLPN_DialPlan302 192.168.4.141 Hangup
(NULL) 2013-08-28 22:28:58 "302" <302> 302 9501 DLPN_DialPlan302 192.168.4.141 Hangup
(NULL) 2013-08-28 22:29:56 "302" <302> 302 9505 DLPN_DialPlan302 192.168.4.141 Dial
(NULL) 2013-08-28 22:30:05 "302" <302> 302 9505 DLPN_DialPlan302 192.168.4.141 Dial
(NULL) 2013-08-28 22:31:31 "302" <302> 302 9505 DLPN_DialPlan302 192.168.4.141 Dial
(NULL) 2013-08-28 22:36:56 "302" <302> 302 9501 DLPN_DialPlan302 192.168.4.141 Playbac
(NULL) 2013-08-28 22:37:02 "302" <302> 302 9501 DLPN_DialPlan302 192.168.4.141 Playbac
(NULL) 2013-08-28 22:38:06 "302" <302> 302 9501 DLPN_DialPlan302 192.168.4.141 Playbac
(NULL) 2013-08-28 22:38:16 "302" <302> 302 9501 DLPN_DialPlan302 192.168.4.141 Playbac
(NULL) 2013-08-28 22:38:31 "302" <302> 302 9505 DLPN_DialPlan302 192.168.4.141 Playbac
(NULL) 2013-08-28 22:39:01 "302" <302> 302 9505 DLPN_DialPlan302 192.168.4.141 Dial
(NULL) 2013-08-28 22:39:24 "302" <302> 302 9505 DLPN_DialPlan302 192.168.4.141 Playbac
(NULL) 2013-08-28 22:40:35 "302" <302> 302 9501 DLPN_DialPlan302 192.168.4.141 Dial

Figura H-3-12

3.6 Configuraciones de Alerta

Después de habilitar las configuraciones de alerta, si el dispositivo fuera atacado, el sistema avisará a los usuarios la alerta vía llamada o e-mail. Los modos de ataque incluyen ataque de IP y web Login.

3.6.1 Ataque IP

Cuando el sistema fue atacado por la dirección IP, el firewall añadirá la IP

automáticamente la Lista Negra de IP y notificará al usuario si corresponda a la regla de protección.
Ejemplo: Configura a notificar la extensión 500, el número saliente es 5503301 y E-mail alert@SISTEK.com.
La configuración pueda ser como las de abajo

Configuraciones de Notificación Telefónica:
Notificación Telefónica: Sí
Número: 500;5503301
Intentos: 1
Intervalo: 60s
Anuncio: Por defecto

Nota: Si hay un número saliente a notificar, el número debe encajar en el patrón marcado de la ruta de salida.

Configuraciones de Notificación E-mail:
Notificación E-mail: Sí
Para: alert@SISTEK.com
Asunto: Ataque de IP

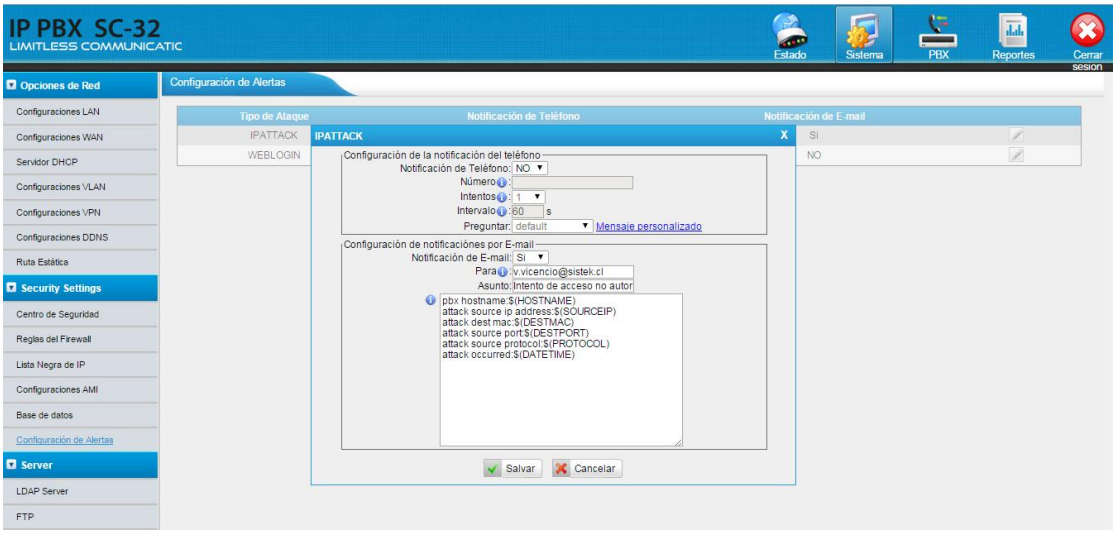


Figura H-3-13

3.6.2 WEBLOGIN

Introduzca la contraseña incorrecta cinco veces a iniciar sesión por Web interfaz de UNI-K será considerando como un ataque, el sistema limitará el inicio de sesión IP en 10 minutos y notificará al usuario.
Ejemplo: Configura a notificar la extensión 500, el número saliente es 5503301 y E-mail alert@SISTEK.com.

La configuración pueda ser como las de abajo

Configuraciones de Notificación Telefónica:

Notificación Telefónica: Sí
Número: 500;5503301
Intentos: 1
Intervalo: 60s
Anuncio: Por defecto

Nota: Si hay un número saliente a notificar, el número debe encajar en el patrón marcado de la ruta de salida.

Configuraciones de Notificación E-mail:

Notificación E-mail: Sí
Para: alert@SISTEK.com
Asunto: WEBLOGIN

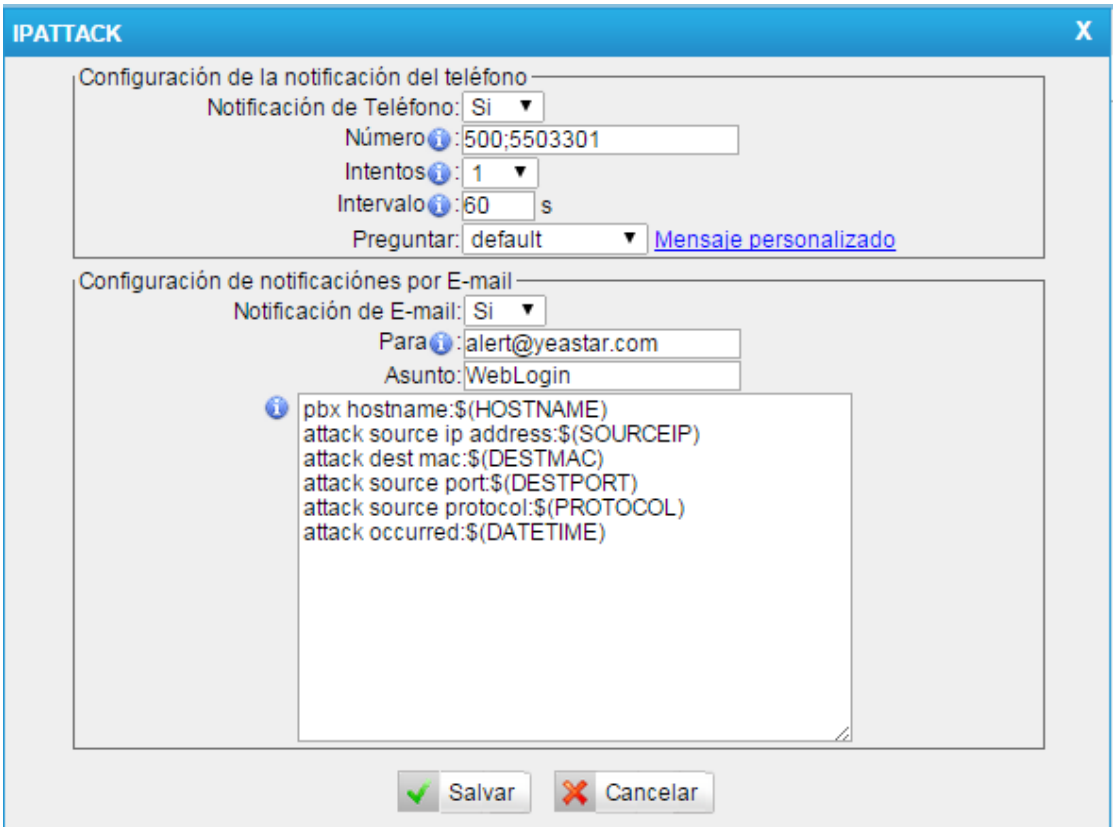


Figura H-3-14

4. Límite de llamada internacional

4.1 Limita crédito de llamada en parte del proveedor

Podemos preguntarle al proveedor de VoIP/PSTN/ISDN para ayudar a limitar el crédito de las llamadas internacionales por adelantado, entonces el hacker no puede marcar las llamadas internacionales. Cada proveedor tiene su propia política. Usted también puede pedir proveedor para desactivar la llamada internacional si no necesario.

4.2 Configura contraseña para la llamada internacional

UNI-K le permite a configurar una contraseña para rutas salientes. Clic "PBX→Control Llamada Saliente→ Ruta Saliente".

Por ejemplo, la contraseña que necesite es 5503333.
Patrón de Marcado: 00. <No pierda el punto aquí>
Contraseña: 5503333
Elija la extensión permitida y el troncal hacia el lado derecho como este:

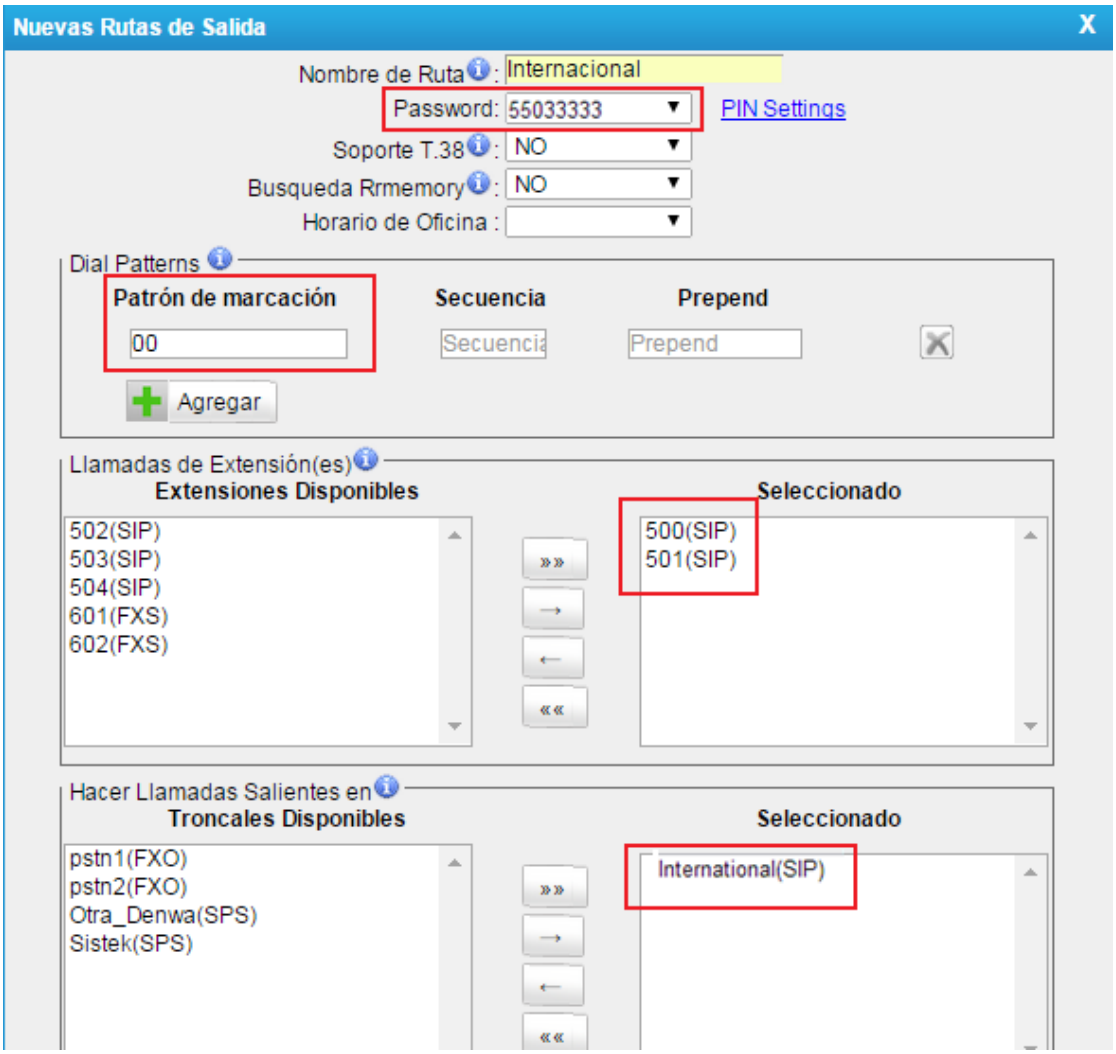


Figura H-4-1

Guarda y aplica los cambios, cuando 300 301 recoge auriculares y marcar un número internacional, UNI-K le pedirá la contraseña, de aprobarse, la llamada será marcada hacia fuera. Si no, la llamada se eliminará.

4.3 Desactiva llamada internacional en UNI-K

Podemos preguntar al proveedor para obtener ayuda a desactivar las llamadas internacionales por adelantado, si no es posible, que podemos configurar las reglas de parte de UNI-K para cortar a todas las llamadas internacionales. Aquí son los pasos detallados:

Paso 1. Crea un troncal de SIP disponible

Crea un troncal de SIP disponible en "PBX→VoIP troncal→Servicio de Proveedor".

La dirección IP puede ser una válida, como 127.0.0.1

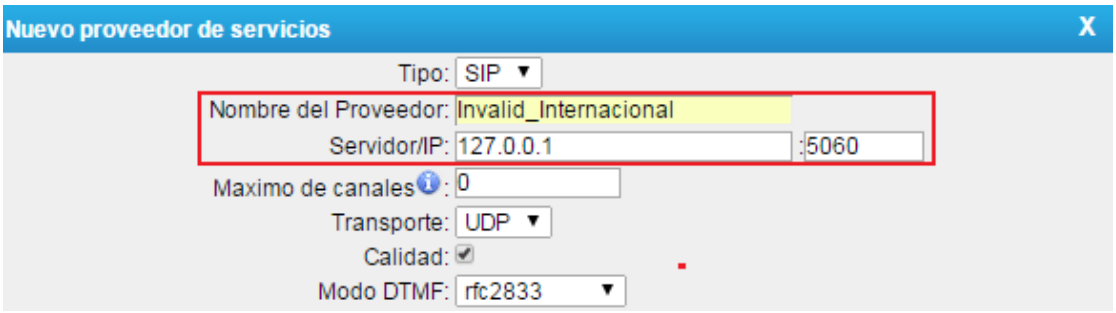


Figura H-4-2

Guarda la y aplica el cambio. El estado de este troncal es inalcanzable por supuesto. Eso es lo que queremos.

Paso 2. Crea una ruta saliente para todas las extensiones y este troncal para rutear llamadas internacionales.

Clic "PBX→Control de llamada Saliente→Ruta Saliente", Crea una nueva:
Nombre: NoInternational
Patrón de Marcado: 00. <No pierda este punto aquí>
Tira: 0
Seleccione todas las extensiones y eso troncal especial (Invalid_international) en el lado derecho.

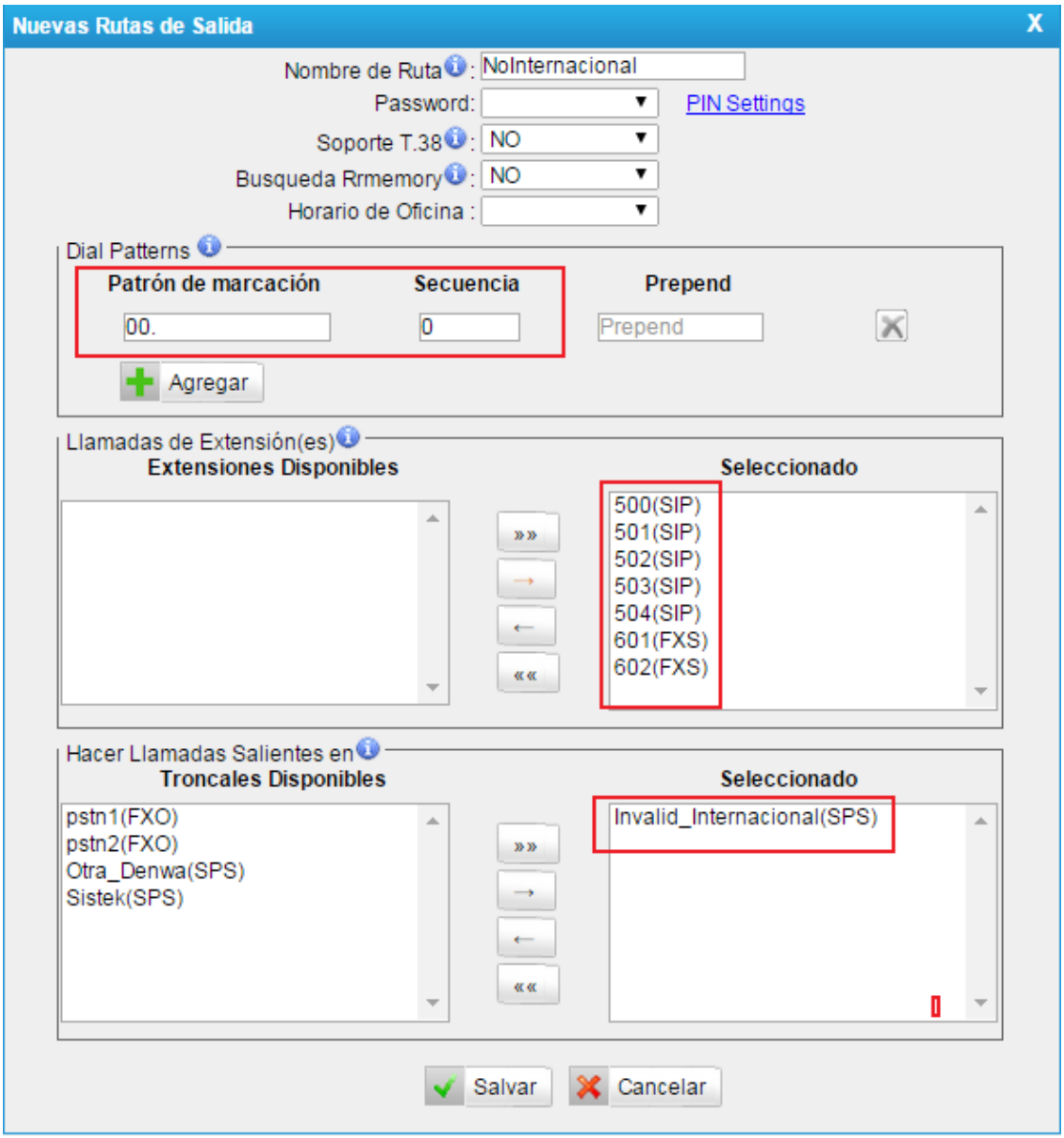


Figura H-4-3

Guarda la y aplica el cambio. Haga clic en la flecha situada a la izquierda para fijarlo a la cima.

Figura H-4-4

En este caso, todas las llamadas internacionales rutarán a este troncal inválido.

Ie. La llamada se corta directamente.

APPENDIX I Cómo Utiliza TLS en UNI-K

I.1 Cómo registra teléfonos IP a UNI-K vía TLS

UNI-K está funcionando como un servidor SIP, teléfonos IP registro a UNI-K como extensiones mediante TLS.

1. Habilita TLS en web interfaz de UNI-K

Clic "→Configuraciones General de SIP de PBX→" a obtener las configuraciones sobre TLS, que está desactivada por defecto. Si usted está usando UNI-K IP PBX SC-32, encontrará en la página "Configuraciones Internas→Configuraciones de SIP".

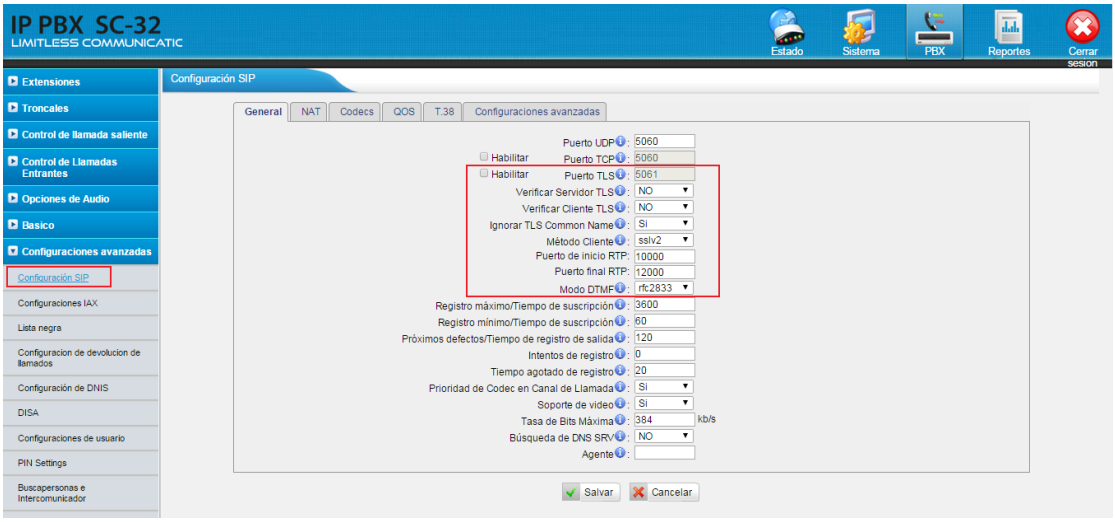


Figura I-1

·TLS Puerto
Puerto se utiliza para registros de SIP, por defecto es 5061.

·TLS Servidor de Compruebe
Cuando utilizando UNI-K como un cliente TSL, sí o no para verificar el certificado del servidor. Es "No" por defecto.

·TLS Cliente de Compruebe

Cuando utilizando UNI-K como un servidor TSL, sí o no para verificar el certificado del servidor. Es "No" por defecto.

·TLS Ignore Nombre Común

Establece este parámetro como "No", y el nombre común debe ser el mismo con IP o el nombre de domain.

·TLS Cliente Método

Cuando utilizando UNI-K como un TLS cliente, especifique el protocolo para la conexión TLS saliente. Puede seleccionarlo como tlsv1, sslv2 o sslv3.

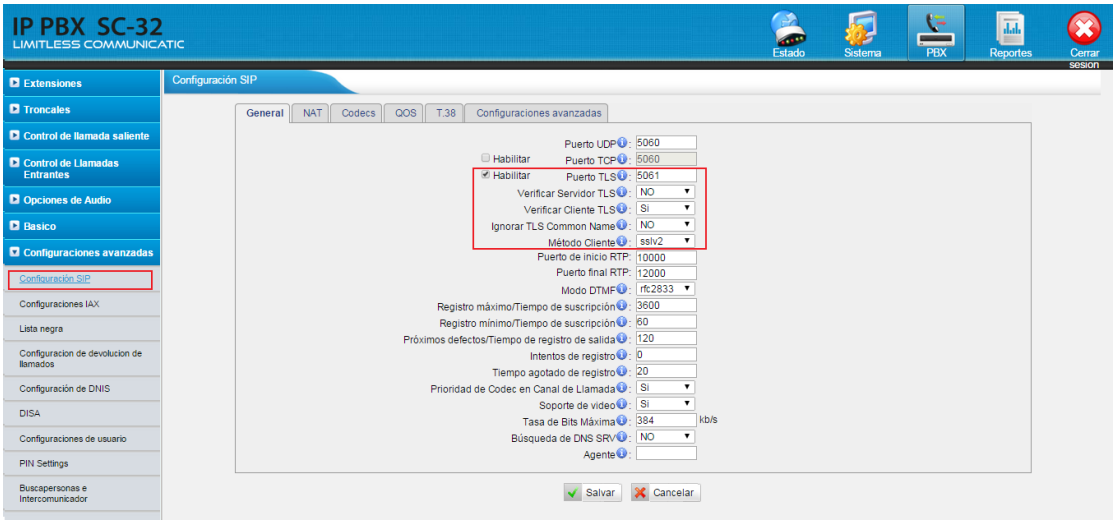


Figura I-2

Notas:

1. Por razón de seguridad, recomendamos a habilitar "TLS verificar cliente" y desactivar "TLS ignorar nombre común", en este caso, UNI-K verificará el certificado de teléfono IP, el nombre común dentro de CA debe ser igual a su IP o nombre de dominio.
2. Método de TLS cliente: es el método TLS de teléfono IP; puede contactar con el fabricante del teléfono IP para conseguirlo.
3. Deberá reiniciar UNI-K para tener efecto después de habilitar TLS.

2. Prepara todos los certificados para TLS

Aquí están los certificados de UNI-K y teléfonos IP para registro TLS como por encima de la pantalla:

CA de UNI-K: CA.crt.
Certificado del servidor de UNI-K: asterisk.pem.
CA del teléfono IP: CA.crt o CA.csr.
Certificado del servidor del teléfono IP: client.pem.

El certificado es generado vía toolkit OpenSSL, puede completar paquetes de recursos desde http://www.openssl.org/, o descarga la herramienta utilizada aquí, link de descarga:
www.unik-latam.com/download/tools/TLS_CA_Tool.rar

Puede encontrar los archivos dentro del paquete como estos:

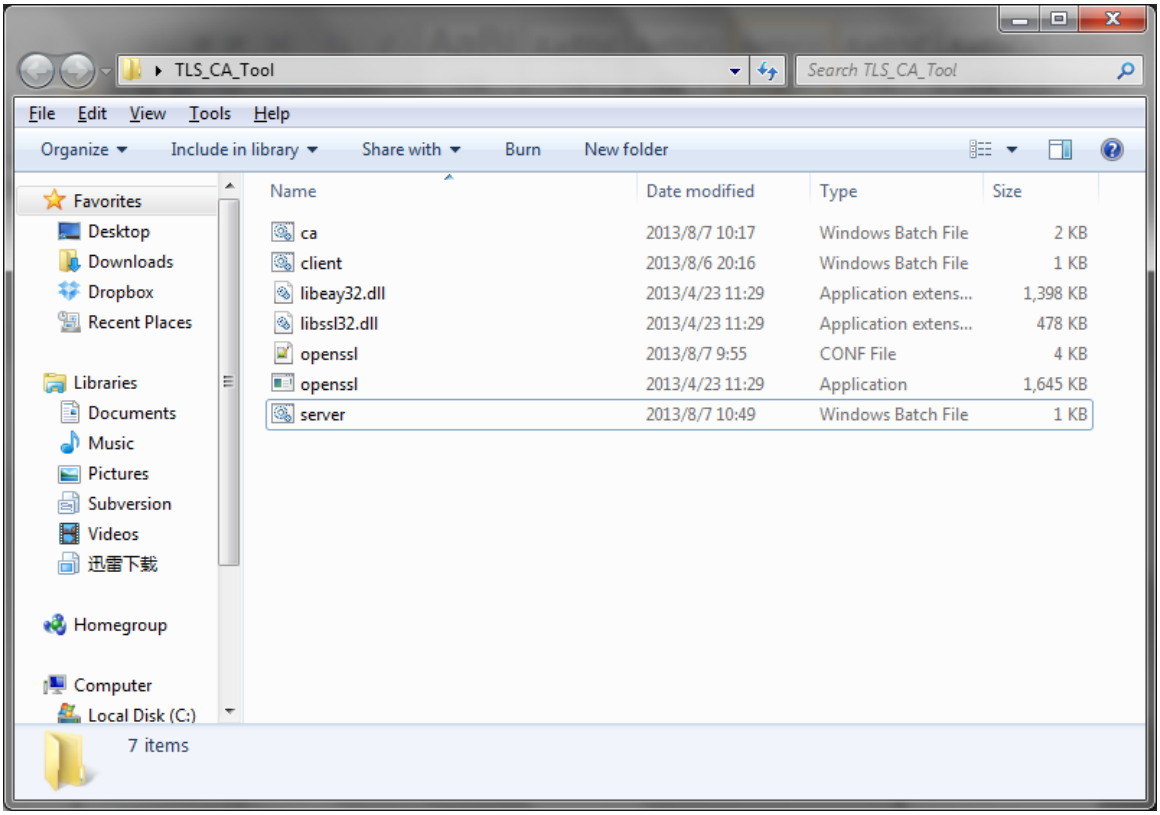


Figura I-3

Ca.bat: Hace el CA.crt para teléfono IP y UNI-K
Client.bat: hace el "client.pem", es el "certificado del servidor del teléfono IP".
Server.bat: hace el "asterisk.pem", es el "certificado del servidor del UNI-K".

Aquí son los pasos a hacer todos los certificados.

Paso 1. Prepara CA de UNI-K: CA.crt.

Doble clic en ca.bat

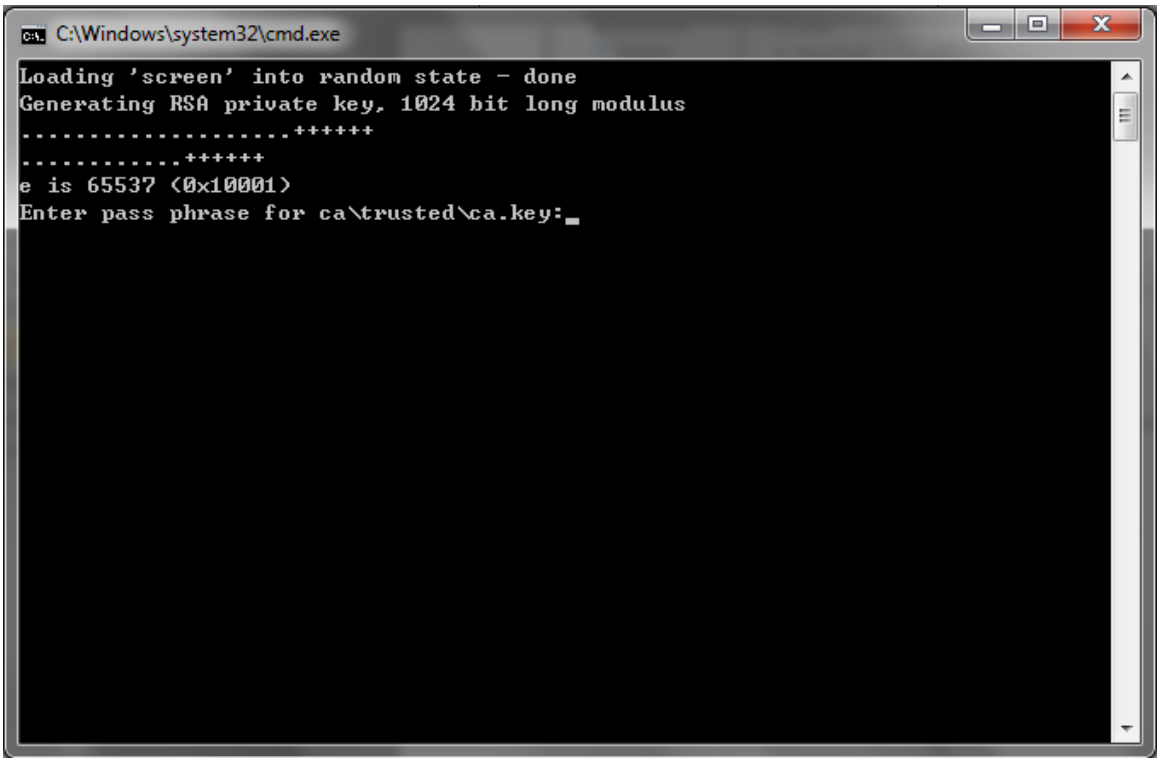
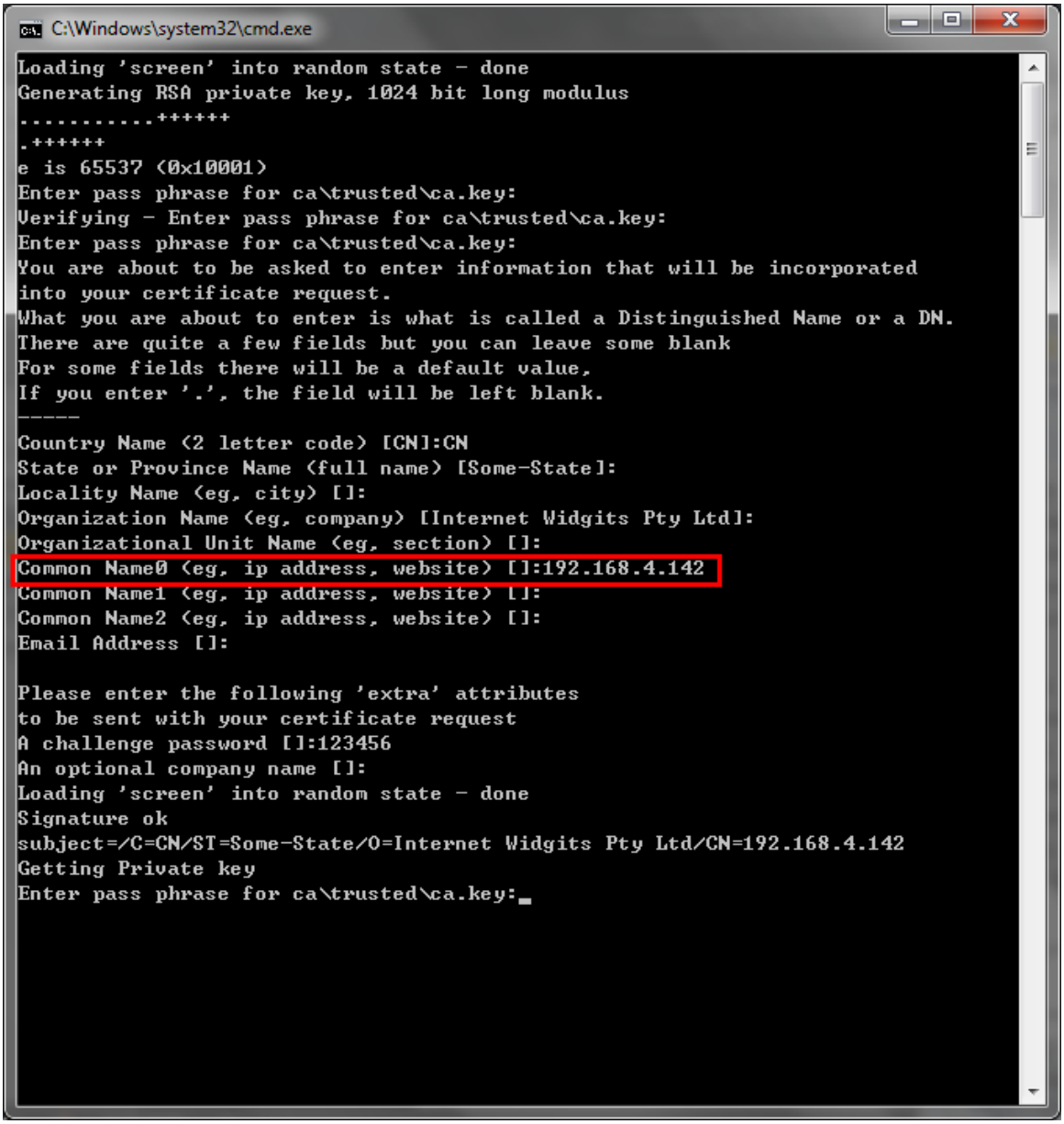


Figura I-4

Sigue la guía para introducir la información de UNI-K paso a paso.
En este ejemplo, la dirección IP de UNI-K es 192.168.4.142.


C:\Windows\system32\cmd.exe
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.....++++++
.++++++
e is 65537 (0x10001)
Enter pass phrase for ca\trusted\ca.key:
Verifying - Enter pass phrase for ca\trusted\ca.key:
Enter pass phrase for ca\trusted\ca.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [CN]:CN
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name0 (eg, ip address, website) []:192.168.4.142
Common Name1 (eg, ip address, website) []:
Common Name2 (eg, ip address, website) []:
Email Address []:
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:123456
An optional company name []:
Loading 'screen' into random state - done
Signature ok
subject=/C=CN/ST=Some-State/O=Internet Widgits Pty Ltd/CN=192.168.4.142
Getting Private key
Enter pass phrase for ca\trusted\ca.key:

Figura I-5

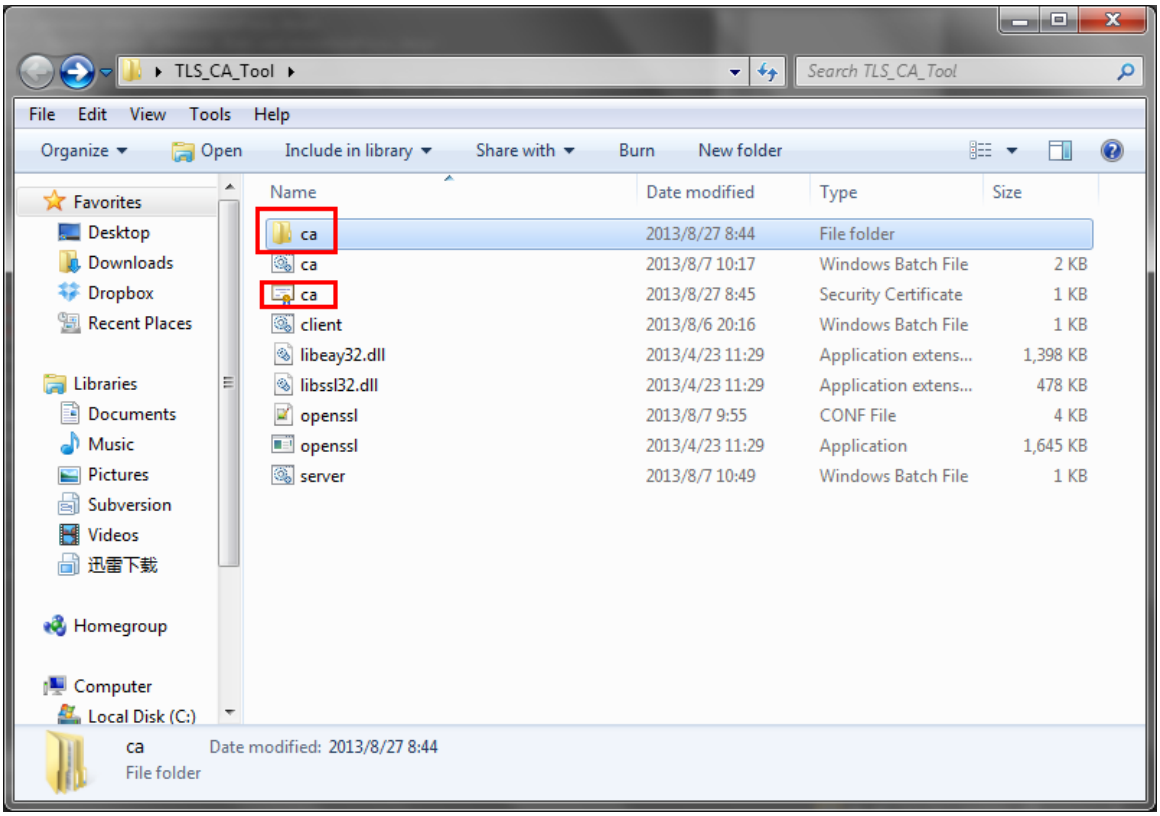


Figura I-6

Este ca.crt es el mismo como el uno en la carpeta /TLS_CA_Tool/ca/trusted/.

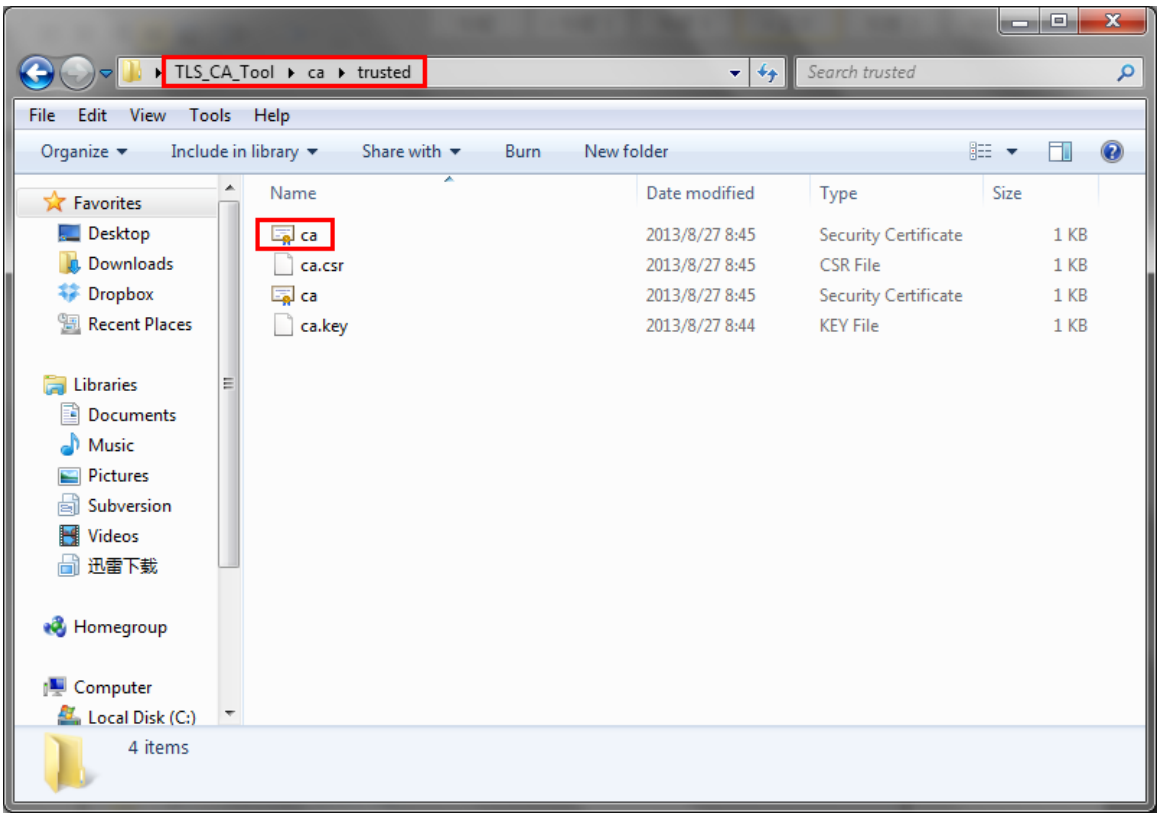


Figura I-7

CA de UNI-K: CA.crt es generado exitosamente.

Paso2 Prepara "asterisk.pem", "Certificado del servidor de UNI-K"

Necesitamos CA.crt y CA.key para hacer certificado del servidor.
Doble clic en "server.bat".

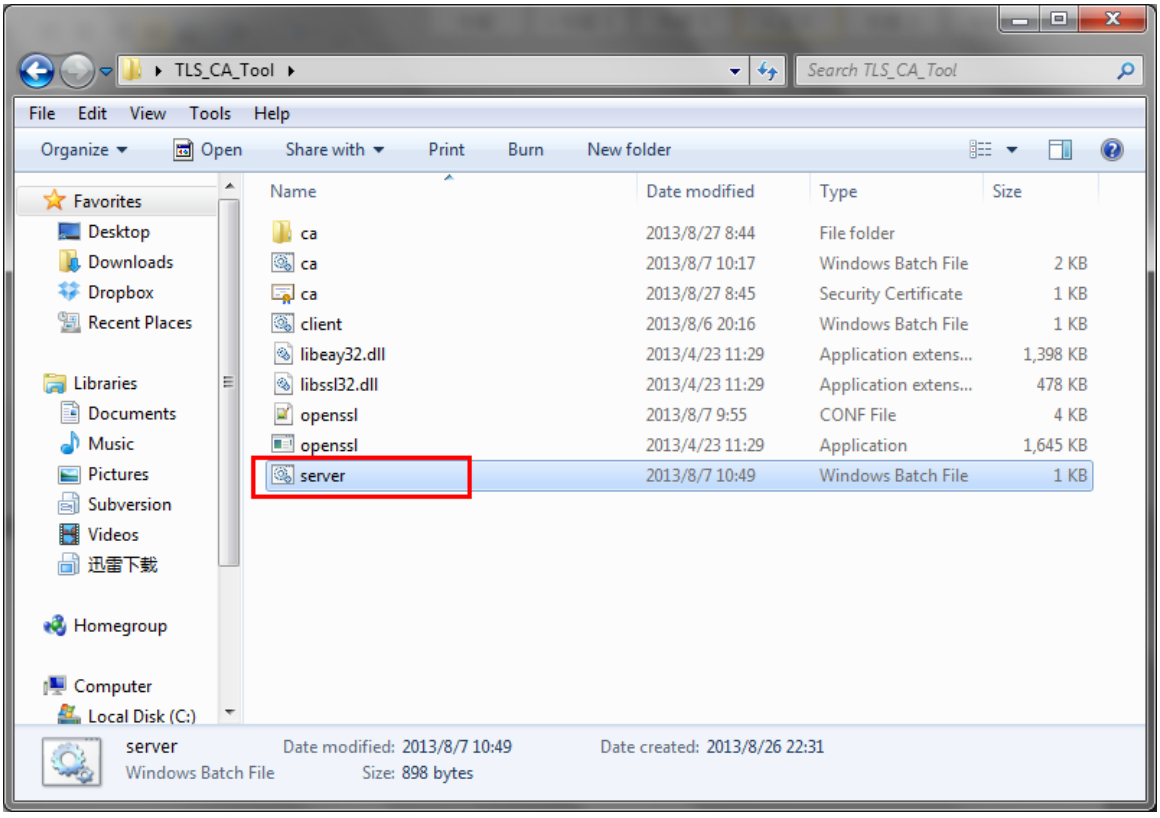
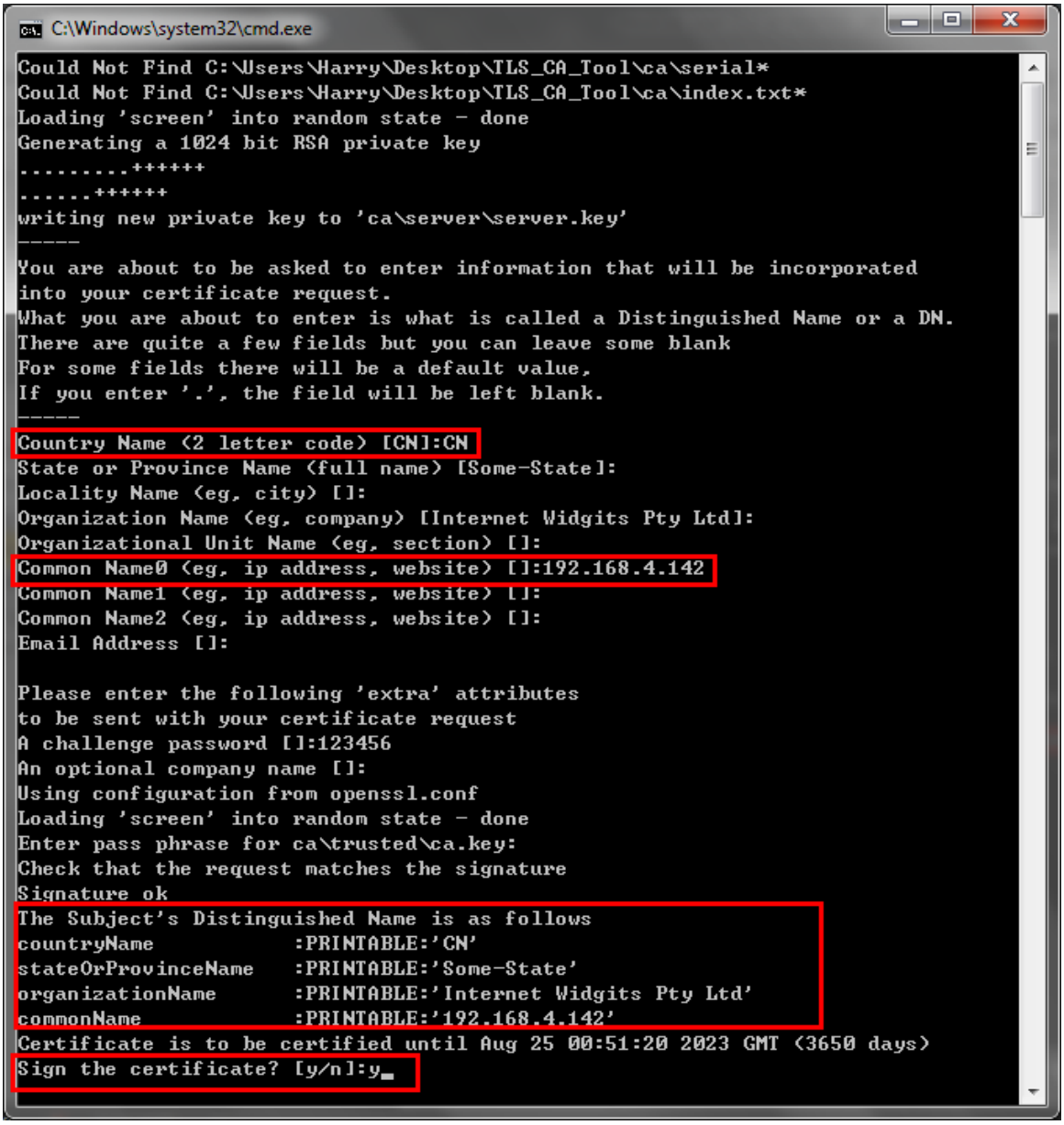


Figura I-8

Siga las guías para ingresar información paso a paso y asegúrese de que la información que ha ingresada coincide con la que ha introducida en Step1.


C:\Windows\system32\cmd.exe
Could Not Find C:\Users\Harry\Desktop\TLS_CA_Tool\ca\serial*
Could Not Find C:\Users\Harry\Desktop\TLS_CA_Tool\ca\index.txt*
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....++++++
.....++++++
writing new private key to 'ca\server\server.key'

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [CN]:CN
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name0 (eg, ip address, website) []:192.168.4.142
Common Name1 (eg, ip address, website) []:
Common Name2 (eg, ip address, website) []:
Email Address []:
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:123456
An optional company name []:
Using configuration from openssl.conf
Loading 'screen' into random state - done
Enter pass phrase for ca\trusted\ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName :PRINTABLE:'CN'
stateOrProvinceName :PRINTABLE:'Some-State'
organizationName :PRINTABLE:'Internet Widgits Pty Ltd'
commonName :PRINTABLE:'192.168.4.142'
Certificate is to be certified until Aug 25 00:51:20 2023 GMT (3650 days)
Sign the certificate? [y/n]:y

Figura I-9

Revisa toda la información luego ingresa "y" a continuar. Cuando termina, usted puede encontrar el asterisk.pem como se muestra en la siguiente imagen.

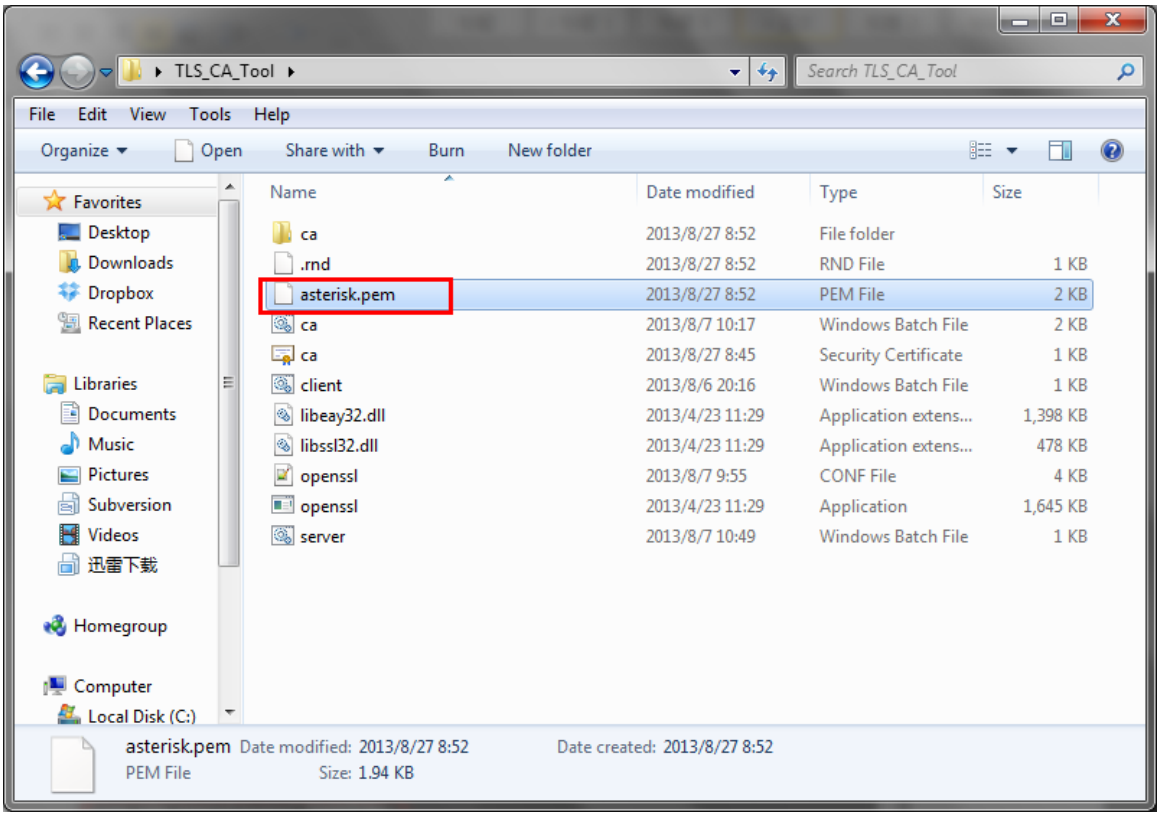


Figura I-10

asterisk.pem, el "certificado del servidor de UNI-K" es generado con éxito.

Nota: Podemos copiar asterisk.pem, ca.crt a otra carpeta antes de hacer el certificado del teléfono IP.

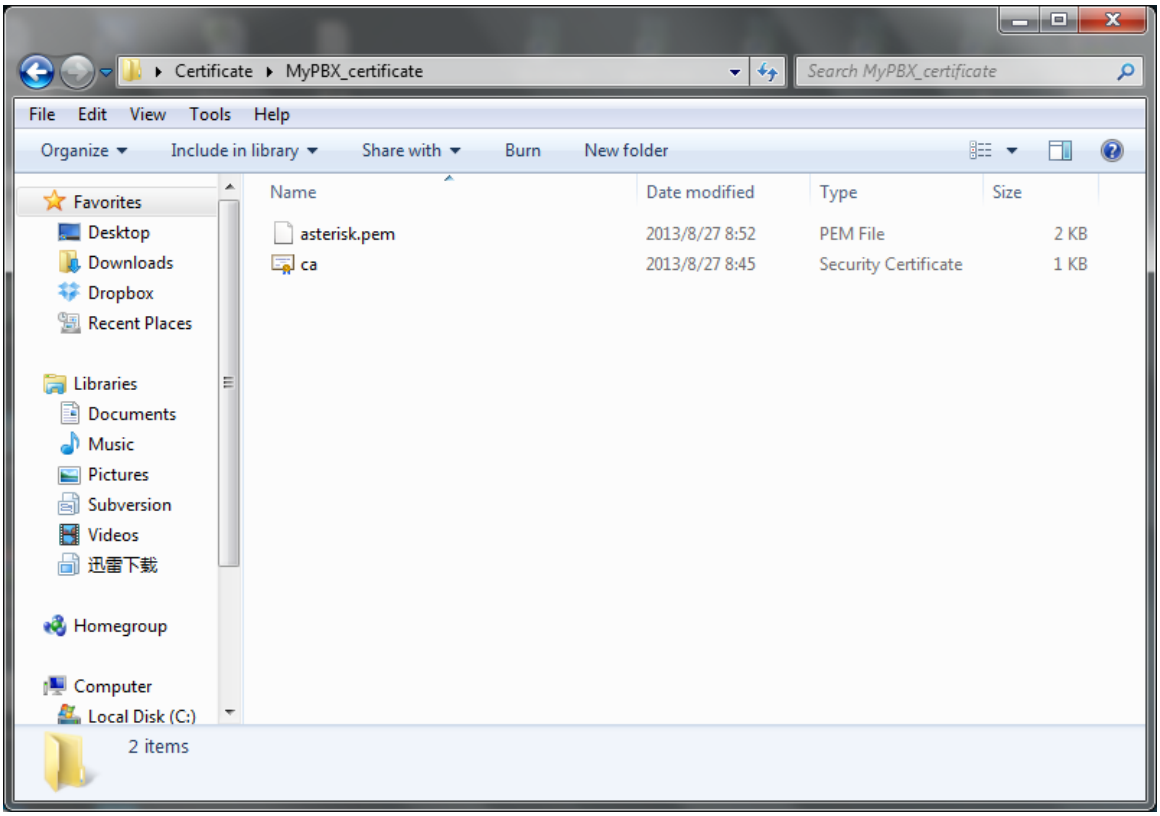


Figura I-11

Paso 3. Prepara el certificado del teléfono IP, cacrt

doble clic en "ca.bat", ingresa la información del teléfono IP paso a paso.

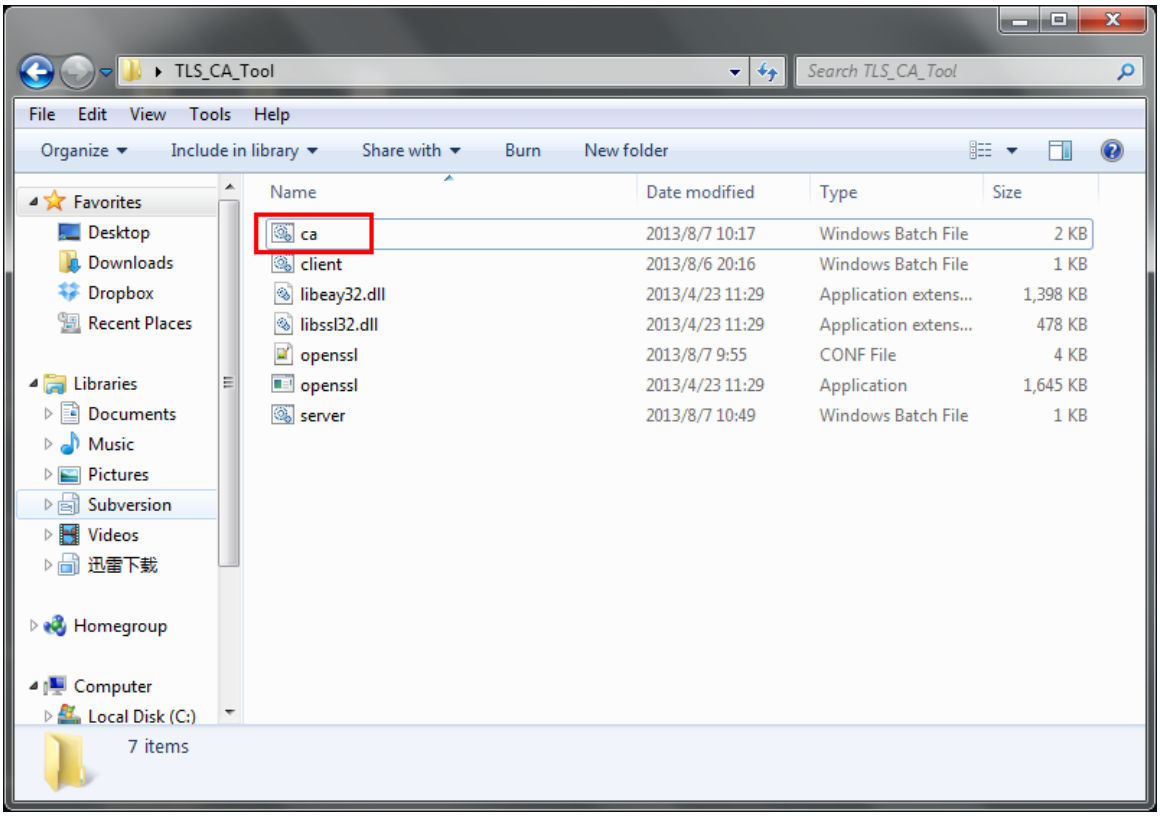
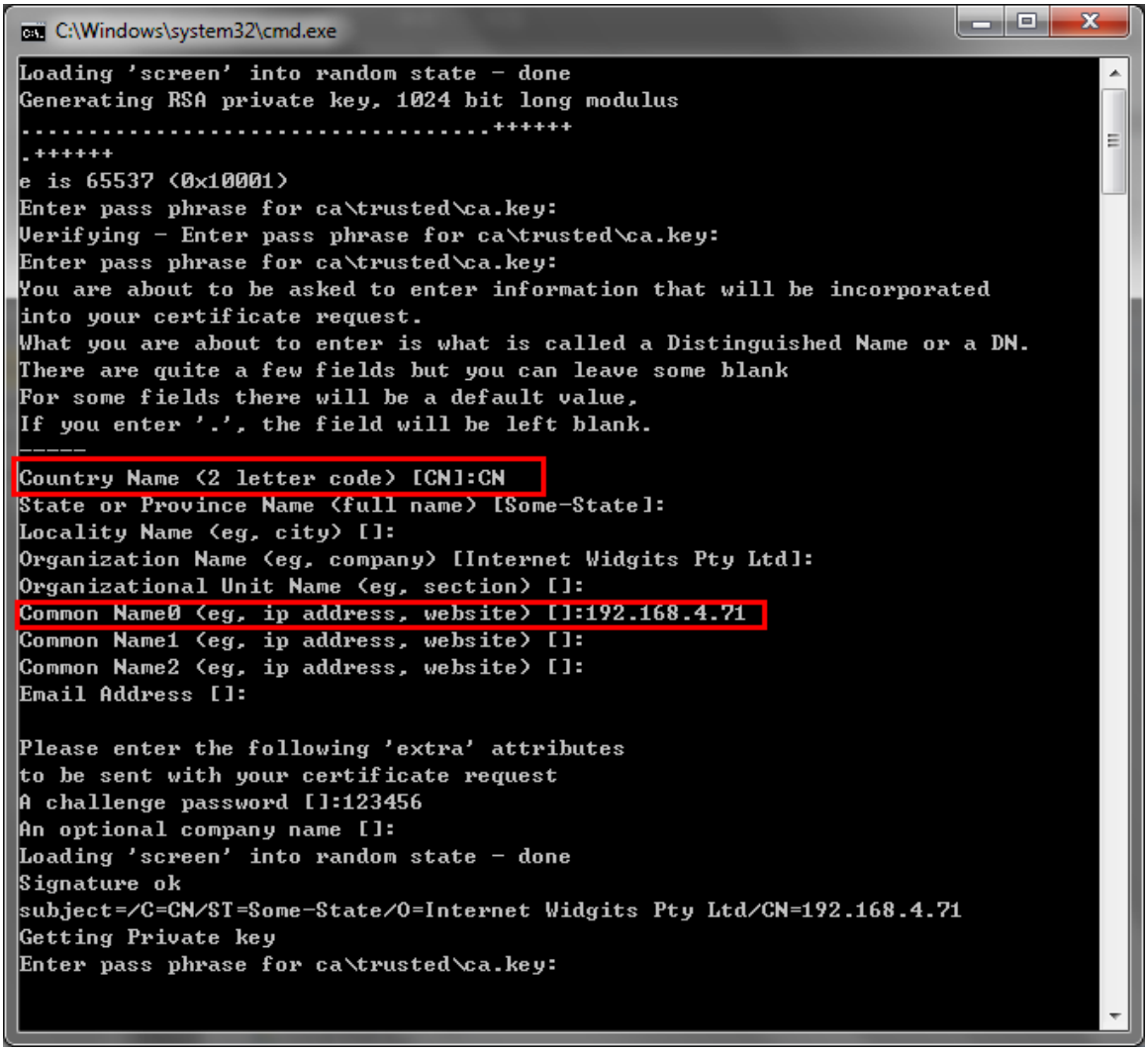


Figura I-12

En este ejemplo, la dirección IP del teléfono IP es 192.168.4.71


C:\Windows\system32\cmd.exe
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.....++++++
.++++++
e is 65537 (0x10001)
Enter pass phrase for ca\trusted\ca.key:
Verifying - Enter pass phrase for ca\trusted\ca.key:
Enter pass phrase for ca\trusted\ca.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [CN]:CN
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name0 (eg, ip address, website) []:192.168.4.71
Common Name1 (eg, ip address, website) []:
Common Name2 (eg, ip address, website) []:
Email Address []:
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:123456
An optional company name []:
Loading 'screen' into random state - done
Signature ok
subject=/C=CN/ST=Some-State/O=Internet Widgits Pty Ltd/CN=192.168.4.71
Getting Private key
Enter pass phrase for ca\trusted\ca.key:

Figura I-13

Cuando termine, podemos encontrar ca.crt en esta carpeta.

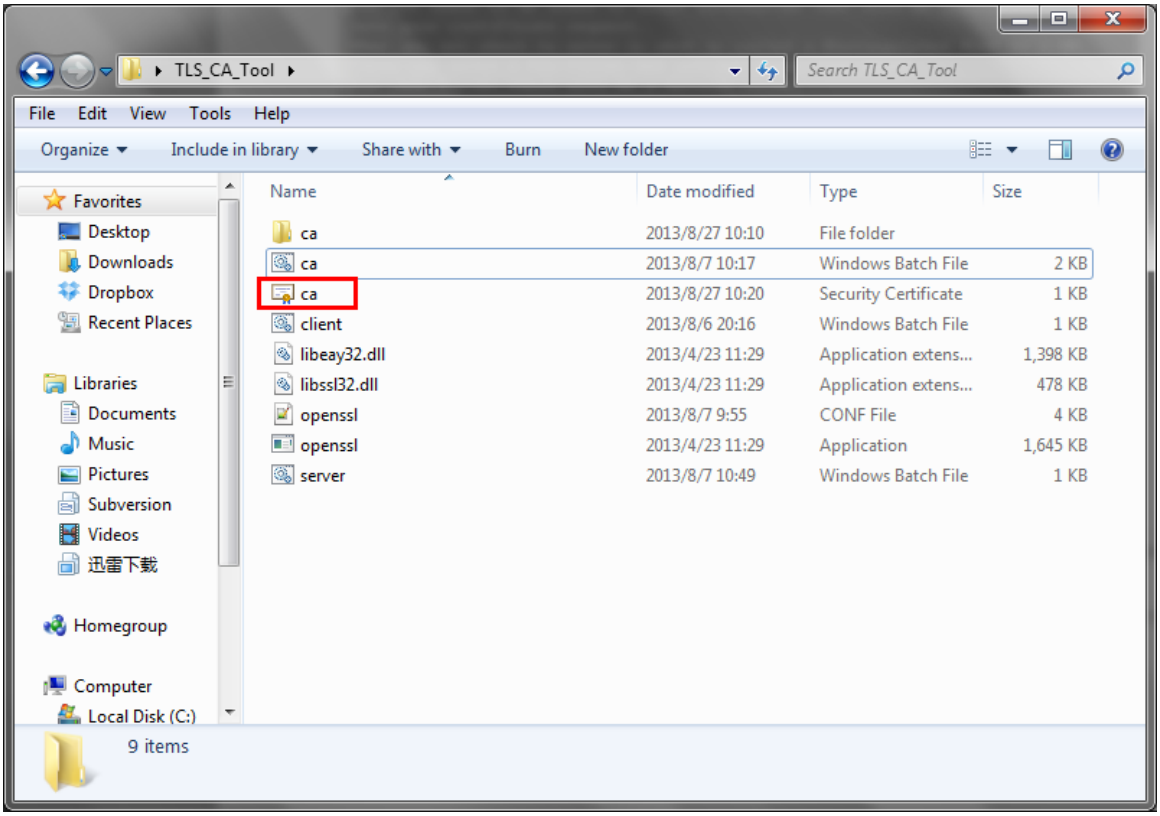


Figura I-14

el ca.crt en folder /TLS_CA_Tool/ca/trusted es el mismo como el anterior.

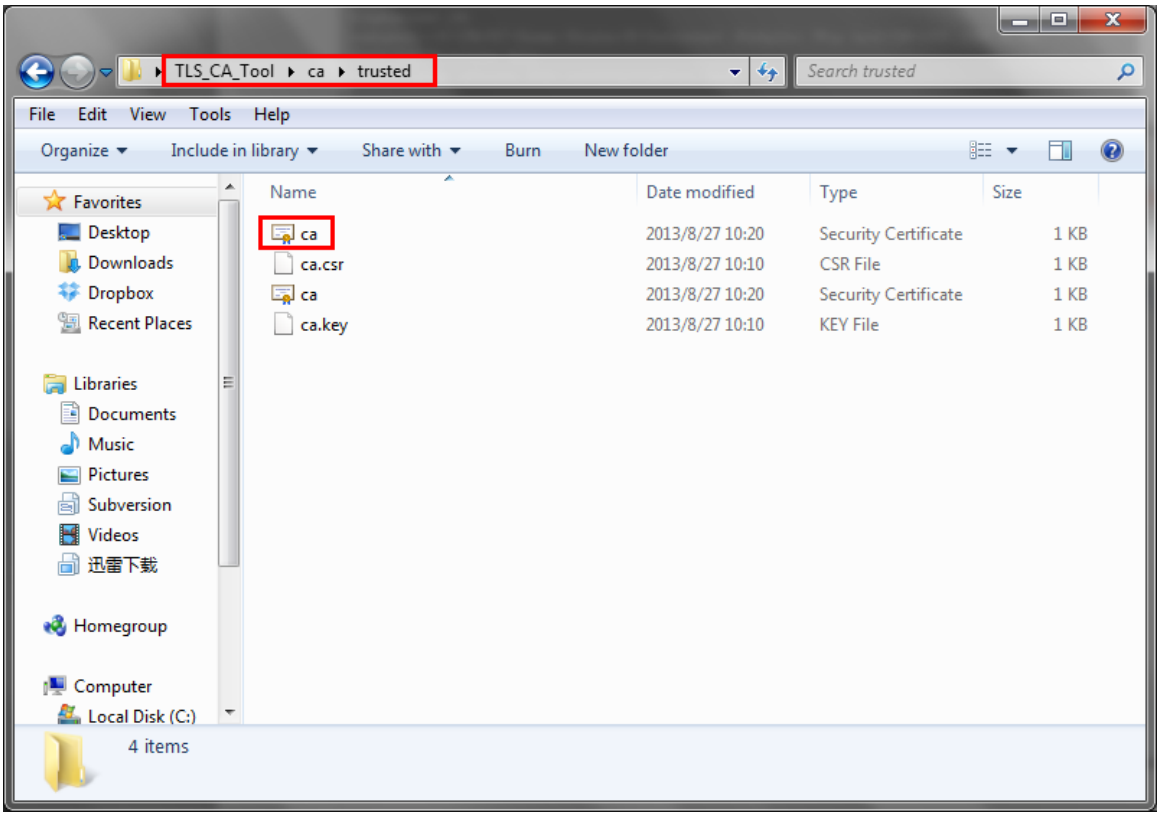


Figura I-15

El certificado del teléfono IP es terminado.

Nota: Si habia conseguido su propio CA para teléfono IP, puede renombrarlo a CA.crt y copiarlo a la carpeta "/TLS_CA_Tool/ca/trusted" antes de hacer el "client.pem".

Paso 4. Prepara "client.pem", el "certificado del servidor del teléfono IP".

Doble clic en "client.bat".

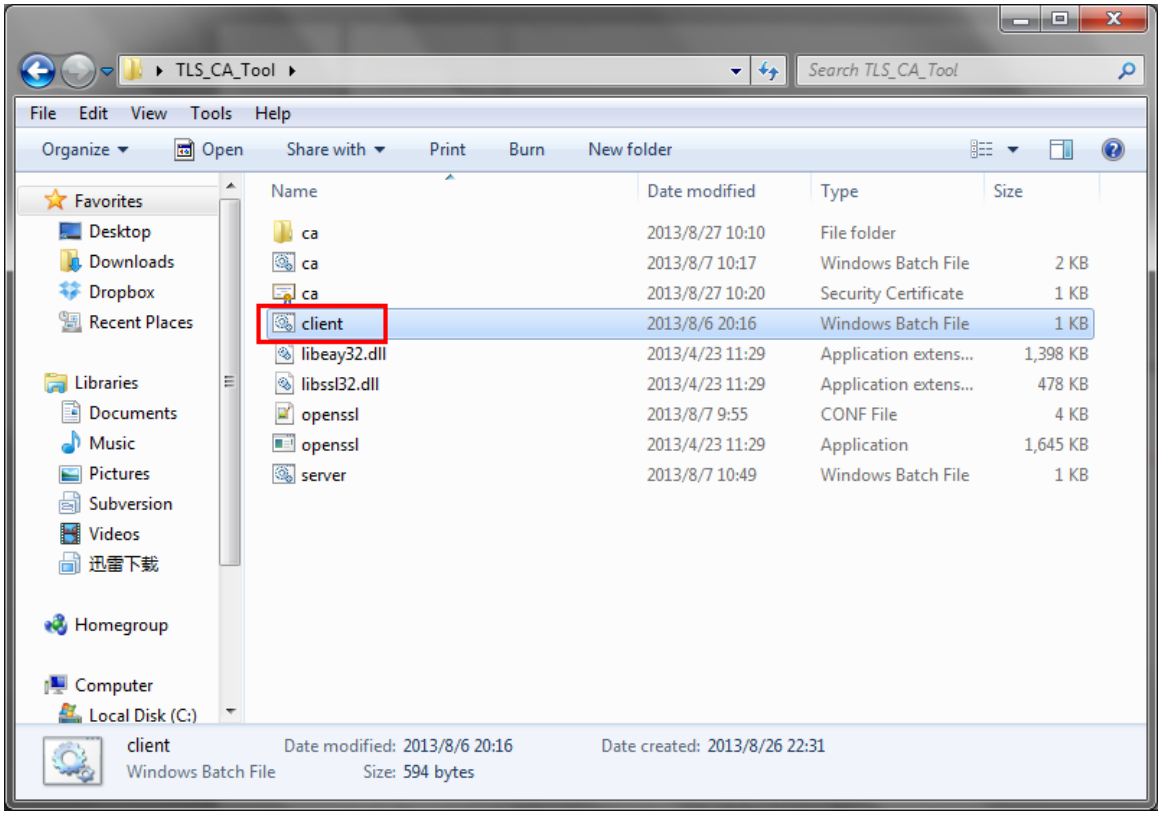
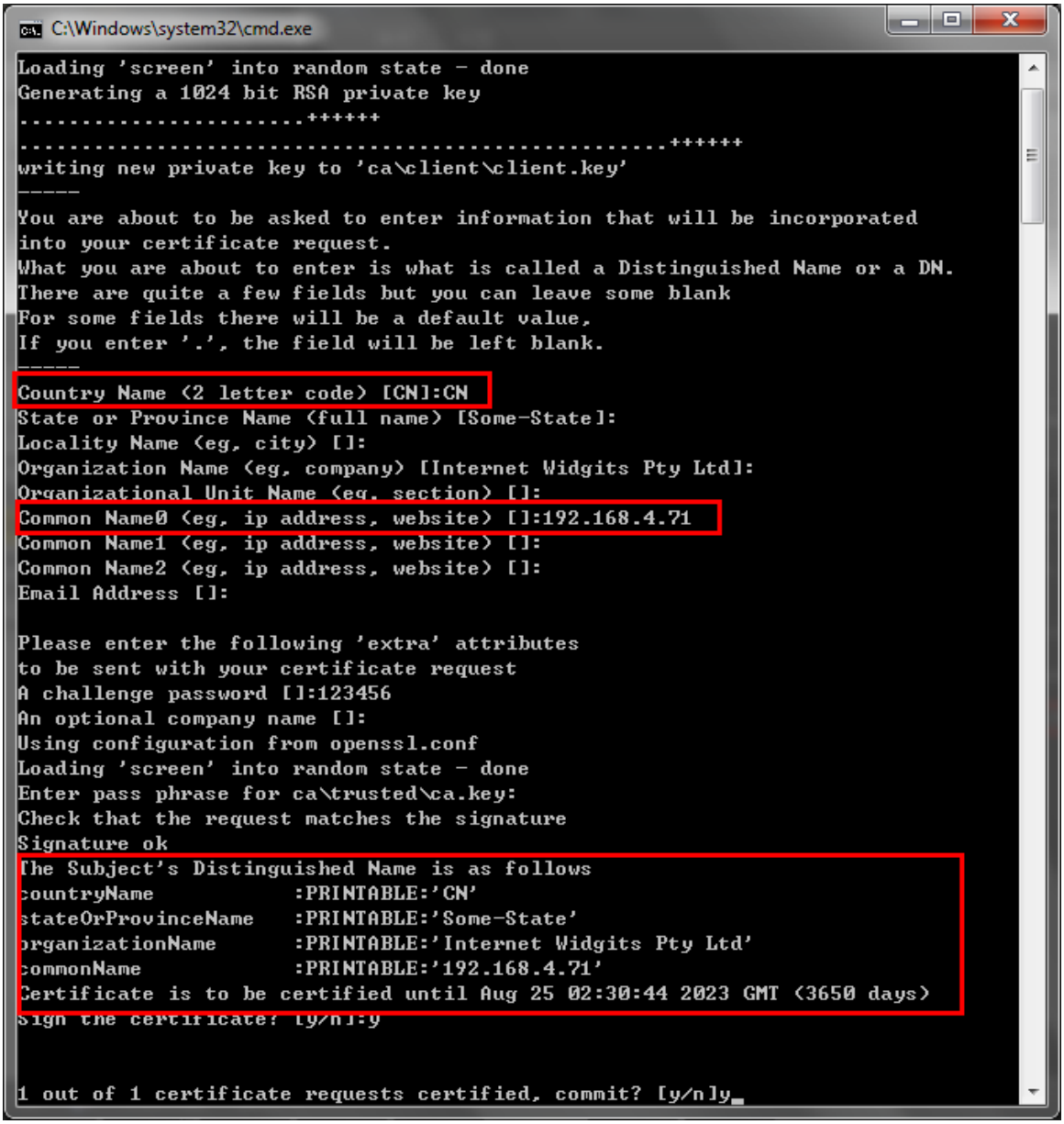


Figura I-16

Ingresa la información del teléfono IP paso a paso en este guión; Asegúrese de que el contenido es el mismo que el Paso3.


C:\Windows\system32\cmd.exe
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....++++++
.....++++++
writing new private key to 'ca\client\client.key'

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [CN]:CN
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name0 (eg, ip address, website) []:192.168.4.71
Common Name1 (eg, ip address, website) []:
Common Name2 (eg, ip address, website) []:
Email Address []:
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:123456
An optional company name []:
Using configuration from openssl.conf
Loading 'screen' into random state - done
Enter pass phrase for ca\trusted\ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName :PRINTABLE:'CN'
stateOrProvinceName :PRINTABLE:'Some-State'
organizationName :PRINTABLE:'Internet Widgits Pty Ltd'
commonName :PRINTABLE:'192.168.4.71'
Certificate is to be certified until Aug 25 02:30:44 2023 GMT (3650 days)
Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified, commit? [y/n]y

Figura I-17

Confirma toda la información que introduzcamos antes de hacer clic en "y" para terminar esta guía.

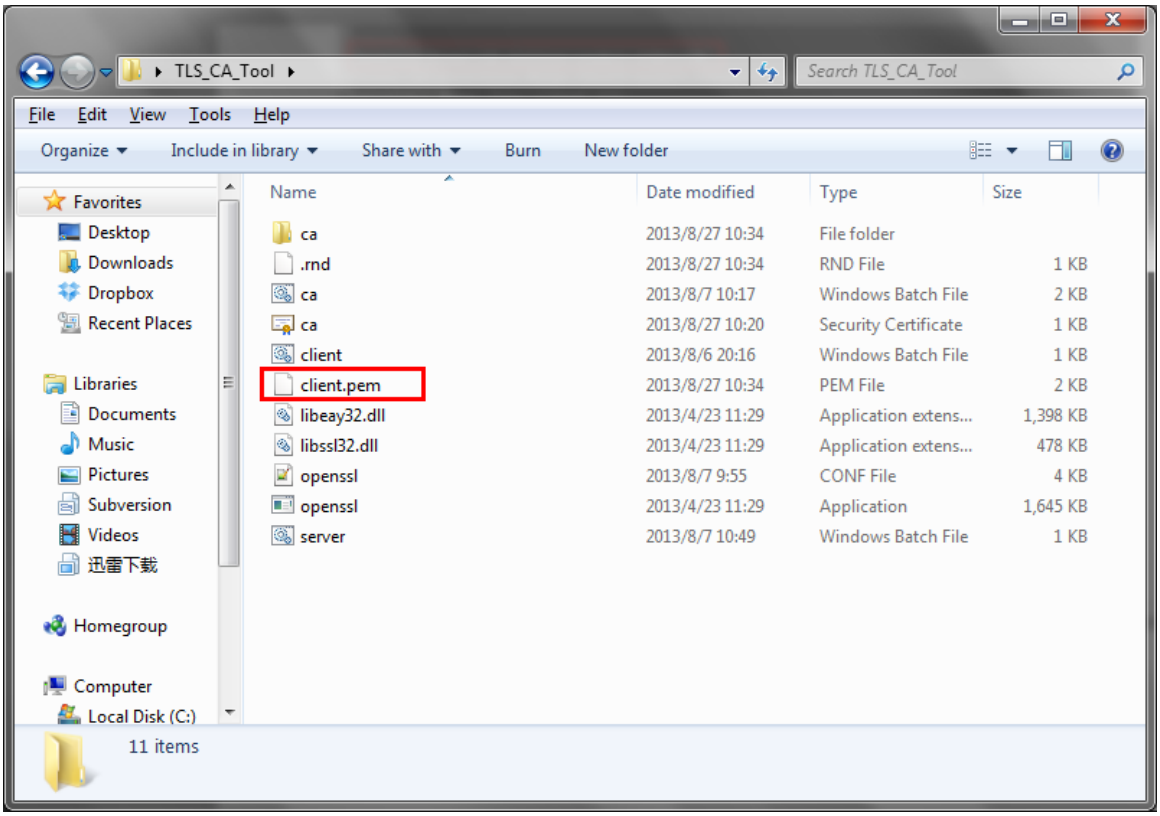


Figura I-18

El “certificado del teléfono IP” está listo.

Nota: Podemos copiar client.pem, ca.crt a otra carpeta antes de la carga.

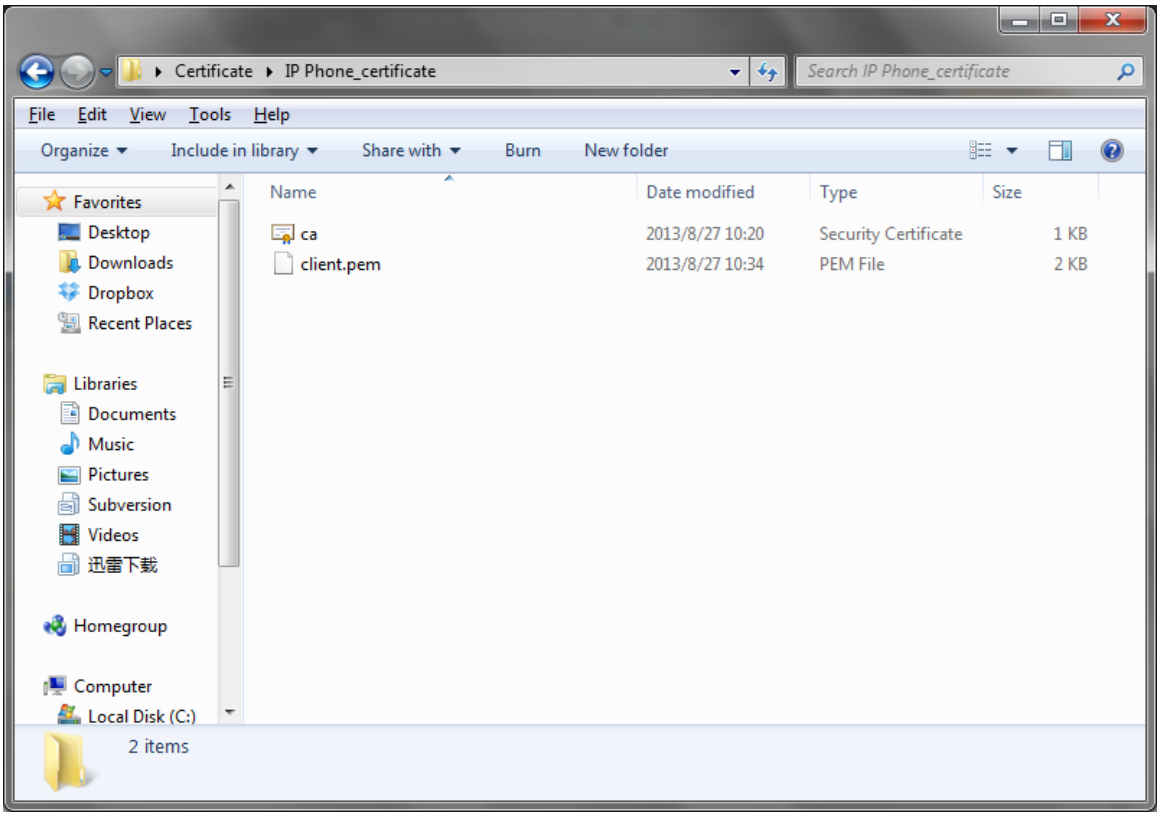


Figura I-19

Todos los certificados son preparados.

3. Carga los certificados

3.1 Carga certificados del teléfono IP

En este ejemplo, El modelo del teléfono IP es Yealink T28.

Paso 1. Carga "certificado del servidor del teléfono IP" (client.pem).

Clic "Seguridad→Certificados del Servidor" a cargar client.pem

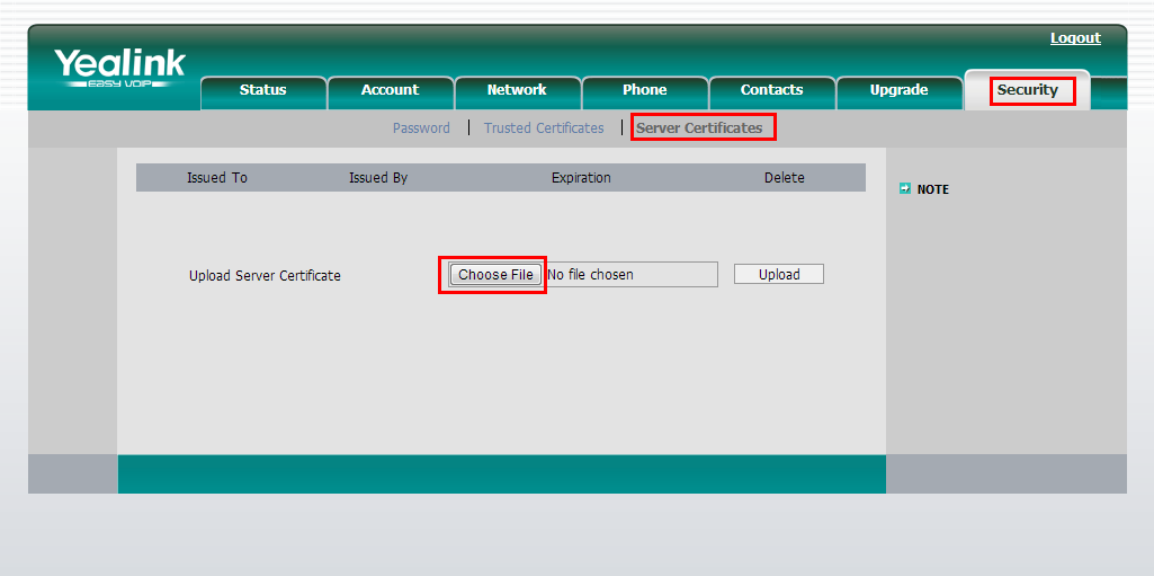


Figura I-20

Clic "Selecciona Archivo" y carga el certificado del servidor del teléfono IP. Teléfono IP reiniciará por sí mismo cuando está cargado con éxito para tener efecto.

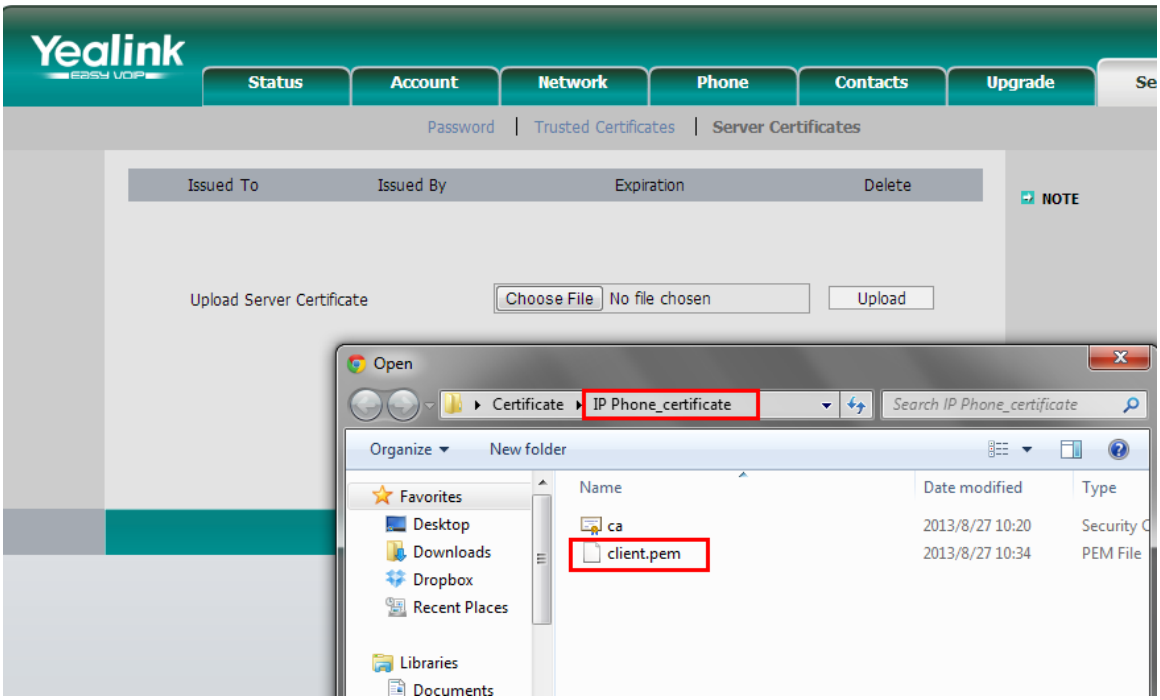


Figura I-21

Cuando teléfono IP arranca otra vez, podemos comprobar el estado del certificado.

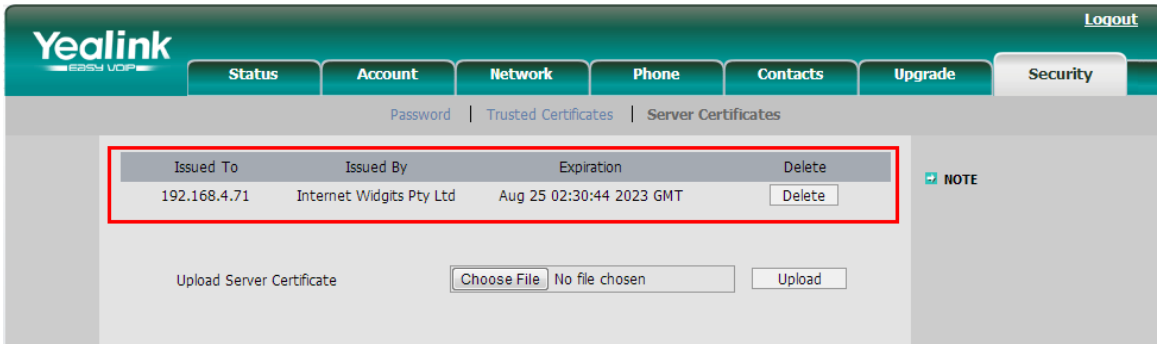


Figura I-22

Paso 2. Carga certificado confiado.

El certificado confiado es ca.crt de UNI-K. Se enviará a UNI-K durante el proceso de registro para obtener una autorización.

Clic "Seguridad→Certificados Confiados", carga ca.crt de UNI-K.

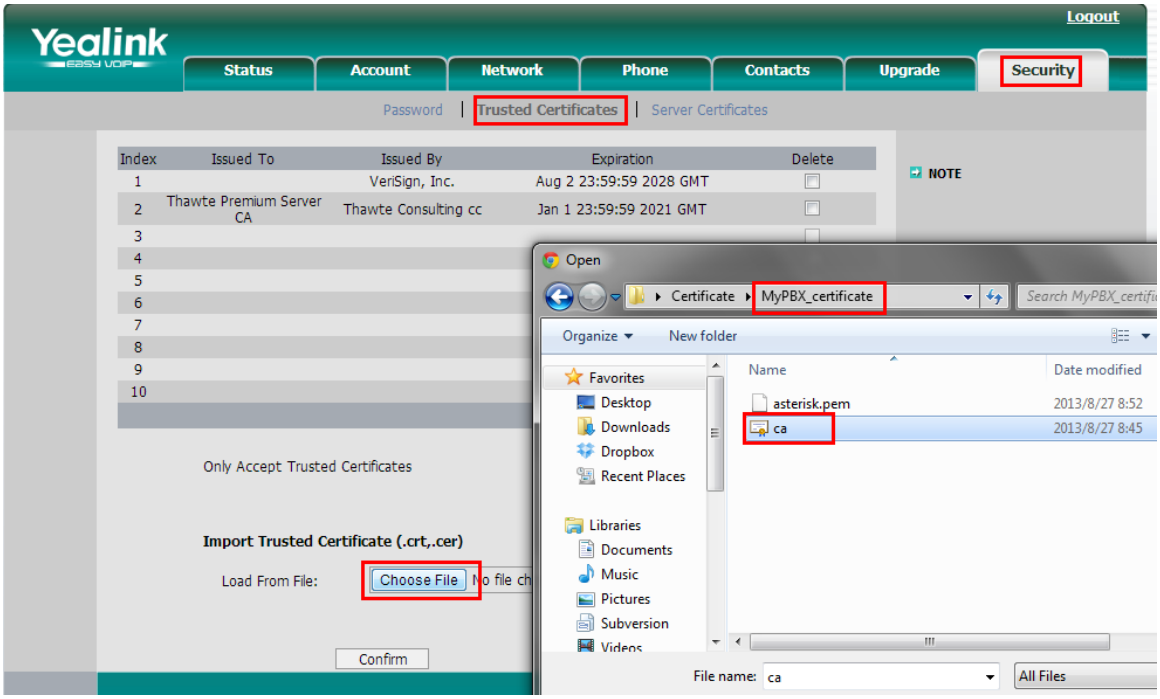


Figura I-23

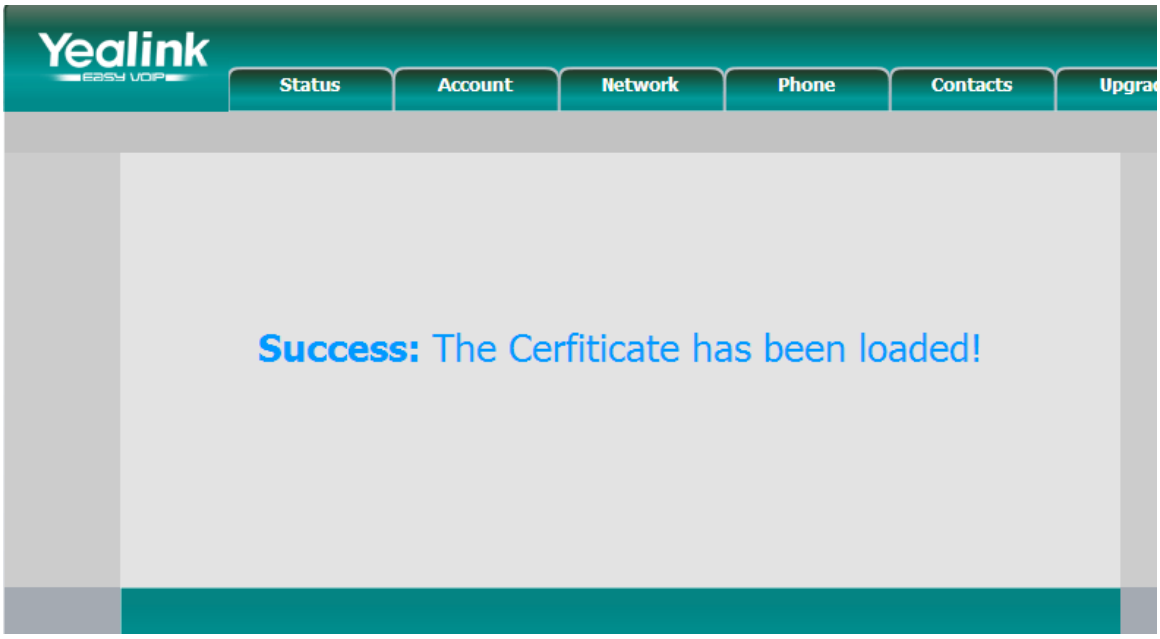


Figura I-24

Cuando termine, podemos comprobar el contenido de CA.crt como en la foto se muestra a continuación.

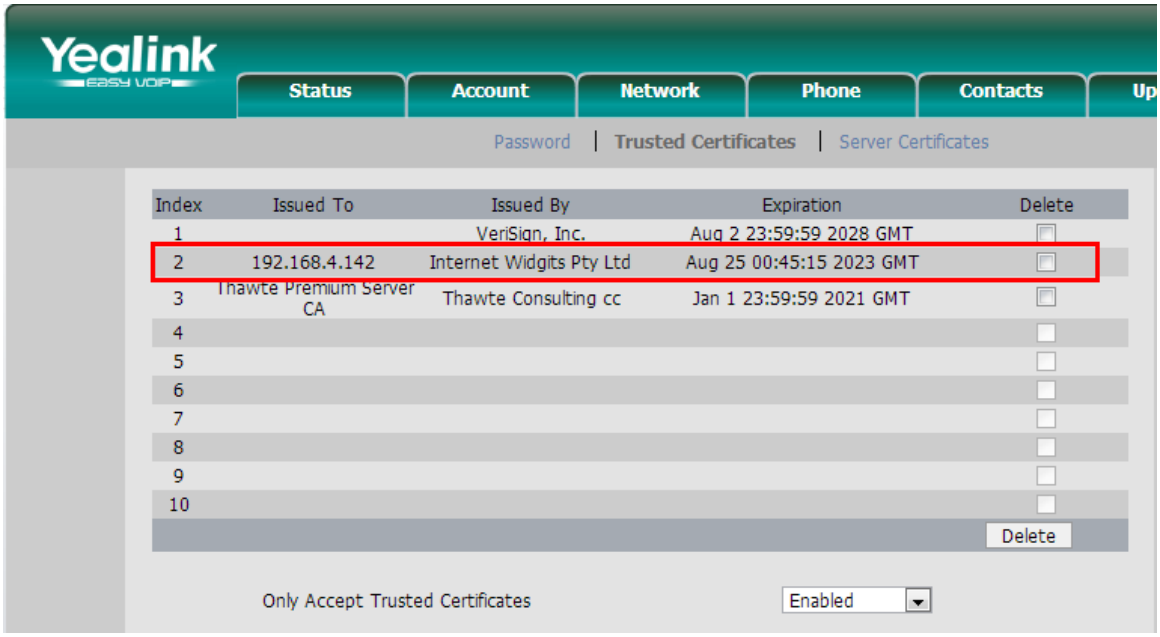


Figura I-25

Los certificados en el lado de teléfono IP están cargados bien.

3.2 Carga certificados de UNI-K

En este ejemplo, el modelo de UNI-K es UNI-K U200 (Versión de firmware: 15.18.0.22)

Paso 1. Carga certificado del servidor de UNI-K (asterisk.pem)

Clic "PBX->Configuraciones Avanzadas->Certificados", luego clic "Carga Certificados", selecciona "certificados de PBX" en tipo windows, luego carga el asterisk.pem.

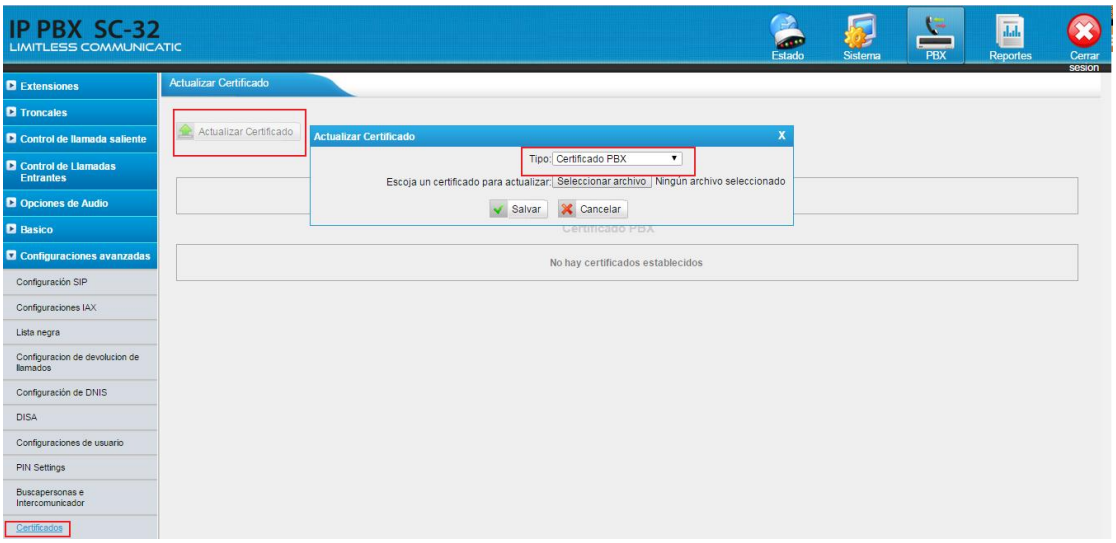


Figura I-26

Clic guarda a cargar, necesitará a reiniciar UNI-K para tener efecto.

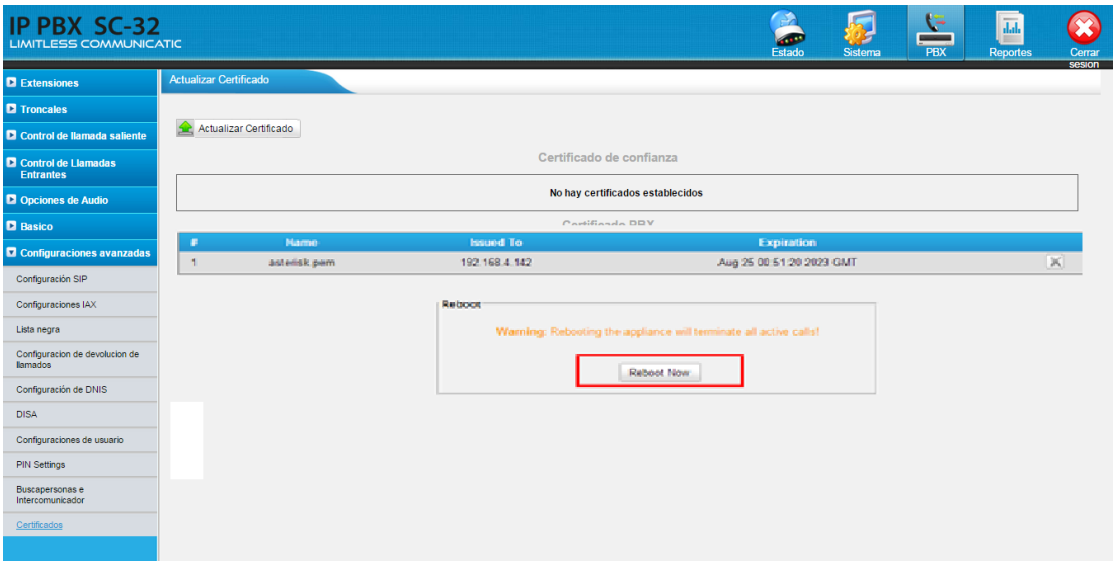


Figura I-27

Clic "Reiniciar Ahora" para reiniciar UNI-K. Cuando termina, podemos mover a Paso 2.

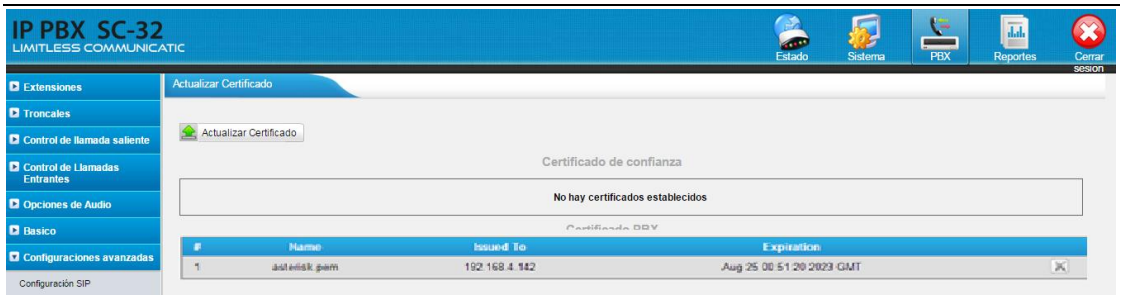


Figura I-28

Paso 2. Carga certificado confiado.

El certificado confiado en UNI-K pude ser el ca.crt del teléfono IP.
Clic "Carga Certificados" y selecciona "Certificados Confiados" en tipo windows, luego carga ca.crt del teléfono IP.

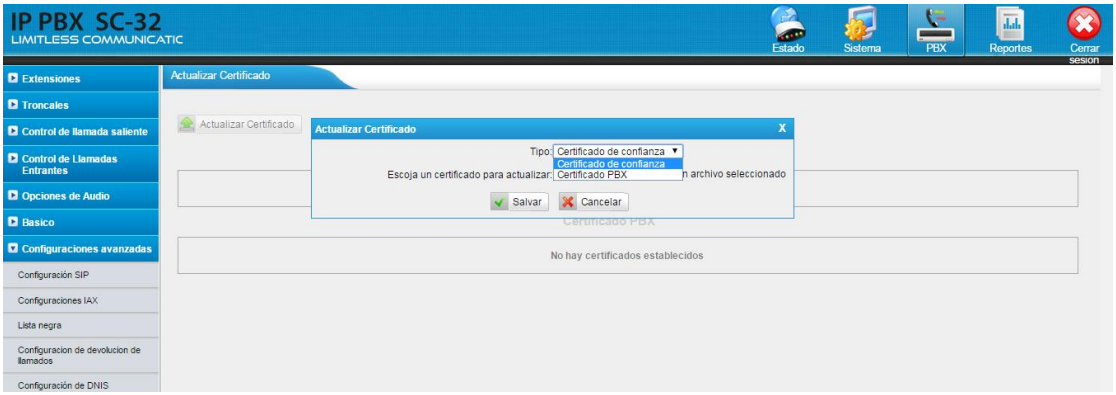


Figura I-29

Clic "Guardar" a cargar, luego clic "Aplica cambios".

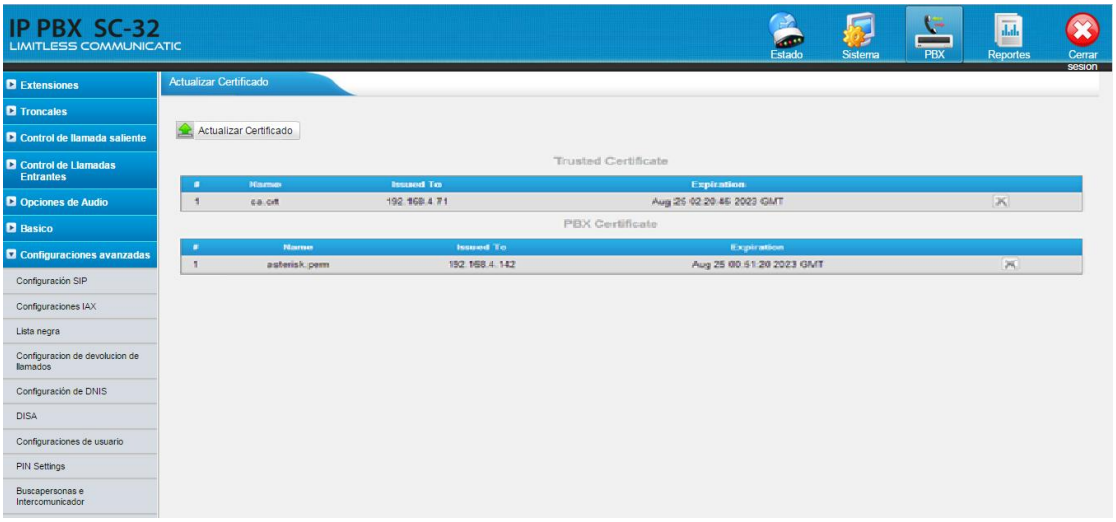


Figura I-30

Los certificados en el lado de UNI-K están cargados bien.

4 Registra teléfonos IP a UNI-K vía TLS

Antes del registra teléfono IP a UNI-K, tenemos que crear una extensión SIP en lado UNI-K por adelantado, o editar una existente. En este ejemplo, el número de la extensión es 303.

Necesitamos establecer protocolo TLS en esta página, haga clic en guardar y "Aplica cambios" en la Web.

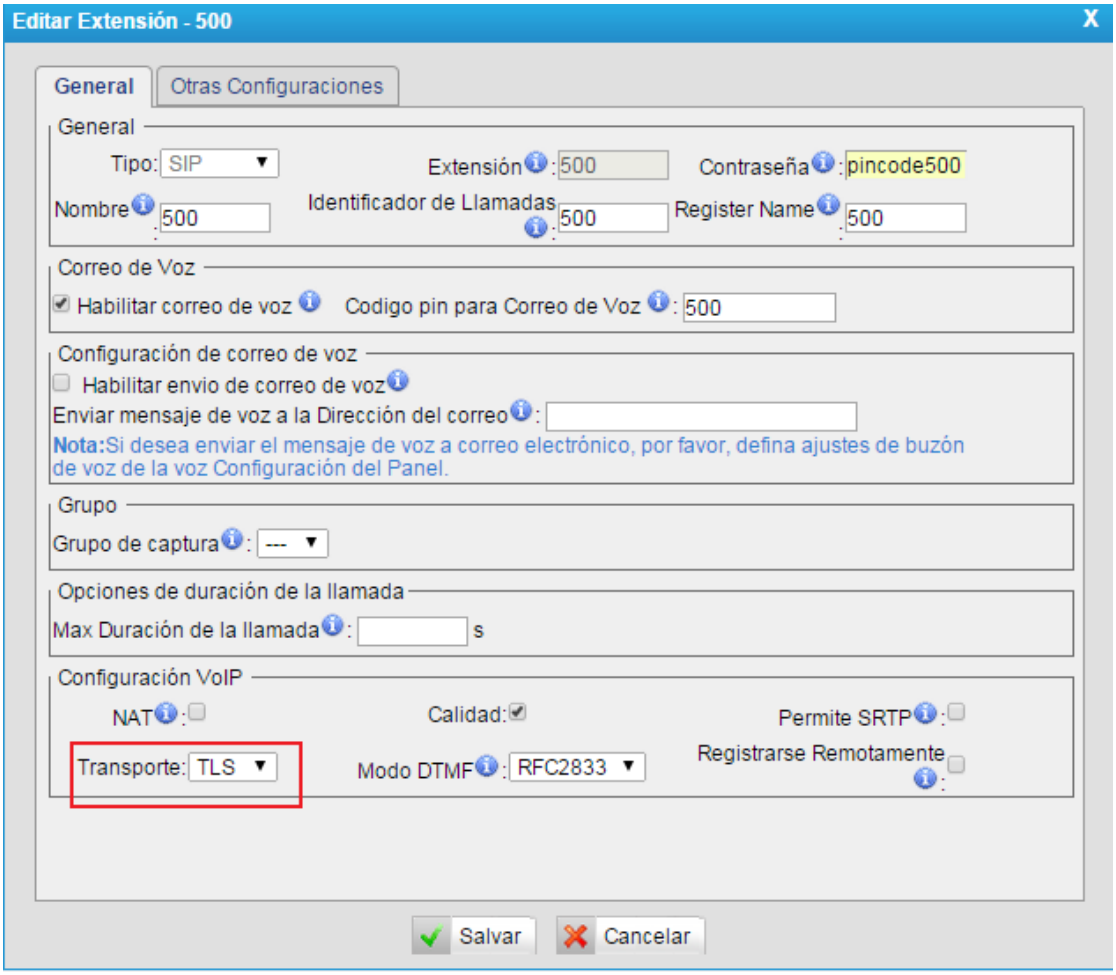


Figura I-31

Abra la página de configuración del teléfono IP, ingrese la información del registro de extensión 303.

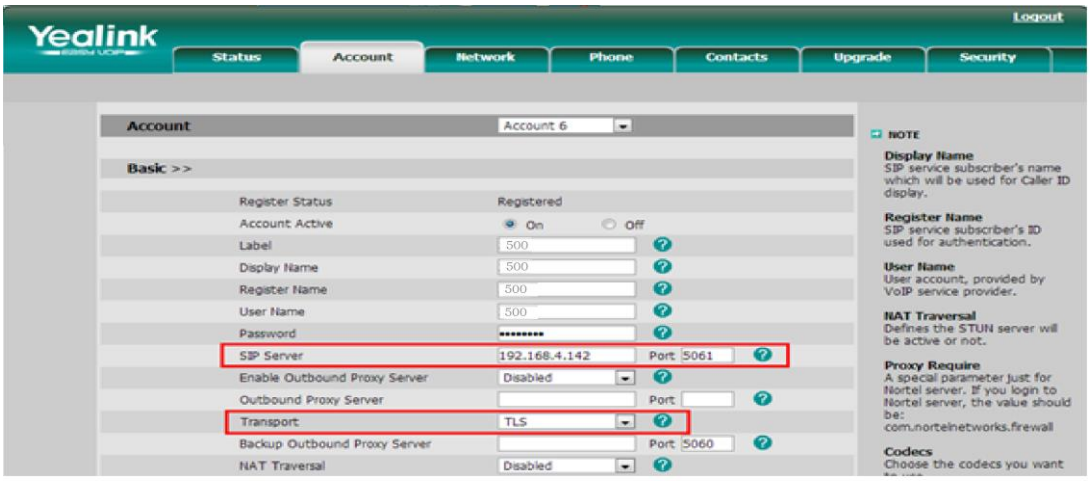


Figura I-32

Clic "Confirmar" para aplicar los cambios, luego la extensión 303 está registrada vía TLS.
También podemos comprobar el estado en la página "Estados" de extensión" de UNI-K.

Figura I-33

Si tiene algún problema sobre el registro de la extensión, por favor rastrea un paquete en "Reportes→Registros del Sistema→Herramienta de Captura Paquete", ingrese la dirección IP del teléfono IP, luego clic en "Empezar". Puede registrar el teléfono IP de nuevo, luego haga clic en "Detener" y descargue el paquete para analizar vía Wireshark. Puede también enviarlo a nosotros para el análisis.

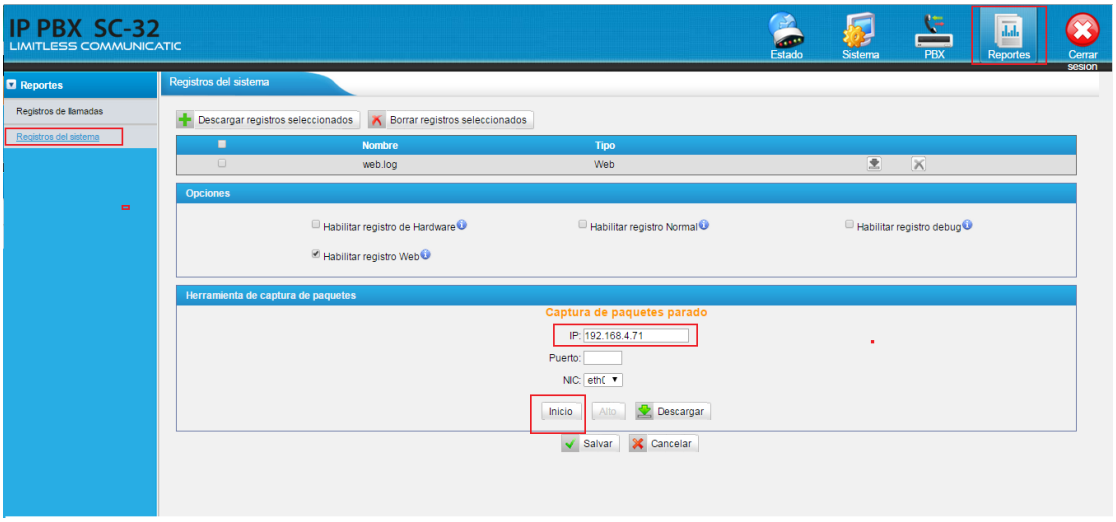

IP PBX SC-32
LIMITLESS COMMUNICATIC
Estado
Sistema
PBX
Reportes
Cerrar sesion
Reportes
Registros de llamadas
Registros del sistema
Registros del sistema
Descargar registros seleccionados
Borrar registros seleccionados
Nombre
Tipo
web.log
Web
Opciones
Habilitar registro de Hardware
Habilitar registro Normal
Habilitar registro debug
Habilitar registro Web
Herramienta de captura de paquetes
Captura de paquetes parado
IP: 192.168.4.71
Puerto:
NIC: eth0
Inicio
Alto
Descargar
Salvar
Cancelar

Figura I-34

I.2 Cómo registra troncal SIP al proveedor VoIP vía TLS

Si habia obtenido el troncal SIP desde el proveedor que está usando TLS, podemos configurarlo en UNI-K y elija TLS dentro del troncal, aquí son dos ejemplos para usted.

VOIP Troncal:

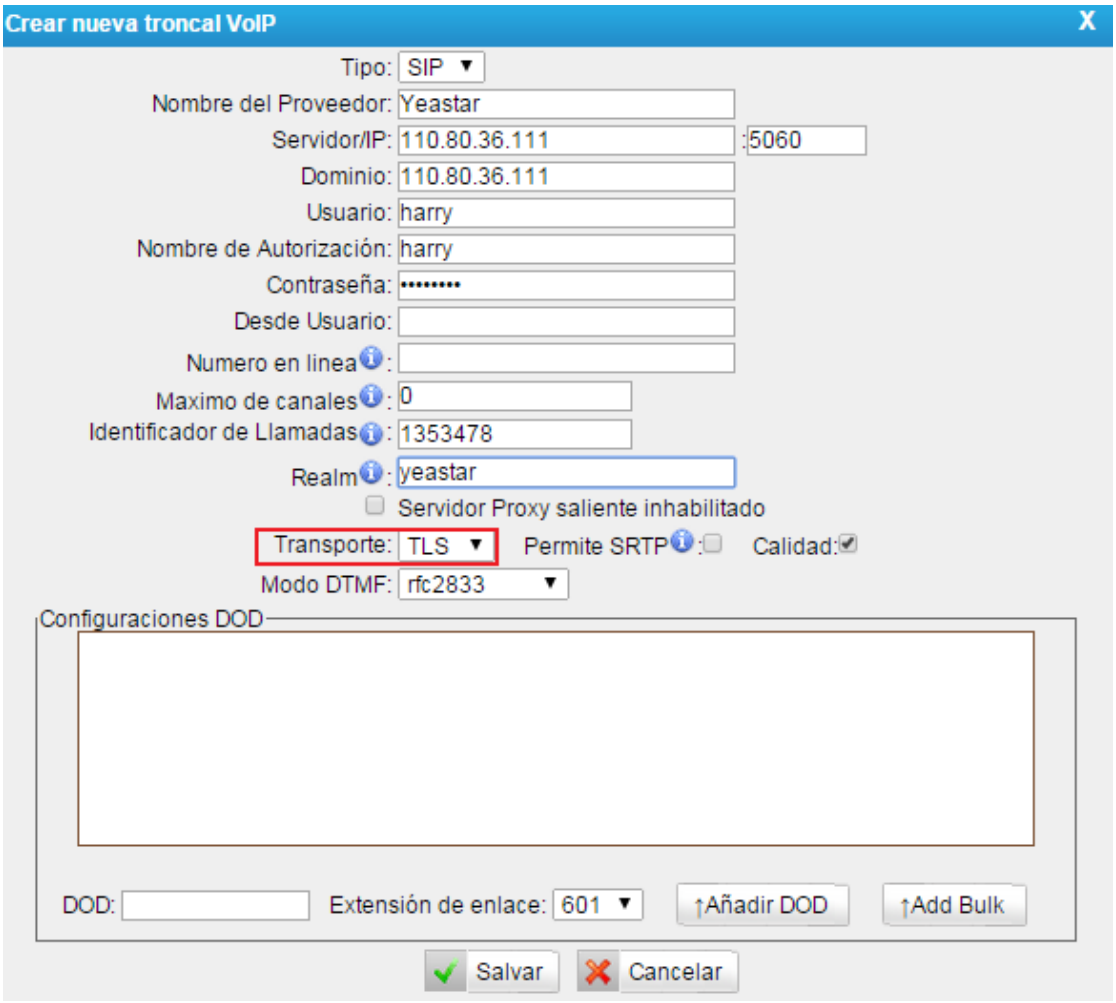


Figura I-35

Troncal del Servicio del Proveedor (P-P).

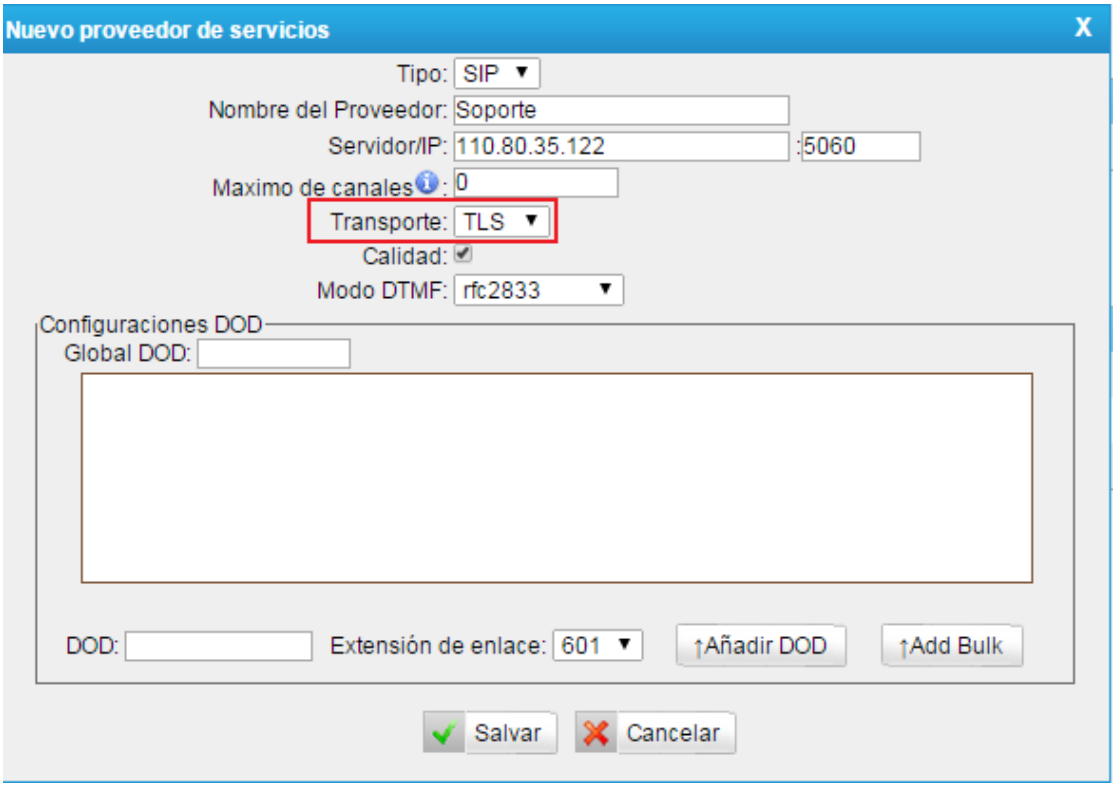


Figura I-36

Si tiene problemas al registrarse al proveedor vía TLS, también puede ejecutar un rastreo de paquetes en la página "Registro del sistema" usando "Herramienta de Captura Paquete", luego enviarlo al proveedor o a nosotros para analizar.

APPENDIX J ¿Cómo Utiliza LDAP?

Estándar LDAP para el protocolo Lightweight Directory Access, que es un protocolo de cliente-servidor para acceder a un servicio de directorio LDAP. Normalmente, LDAP se utiliza como guía telefónica en UNI-K para que pueda buscar una palabra clave desde su teléfono IP.
Aquí tomamos teléfono IP Yealink T-28 como un ejemplo.

1. Configuración en UNI-K.
Marca la opción de "Activa LDAP", y utiliza configuración predeterminada en otros campos.
La configuración predeterminada como abajo:

Root Node: dc=pbx,dc=com
PBX Node: ou=pbx,dc=pbx,dc=com
Nombre de Usuario: cn=admin,dc=pbx,dc=com
Contraseña: (Rellena como requerida)

Luego puede agregar contactos como sea necesario.

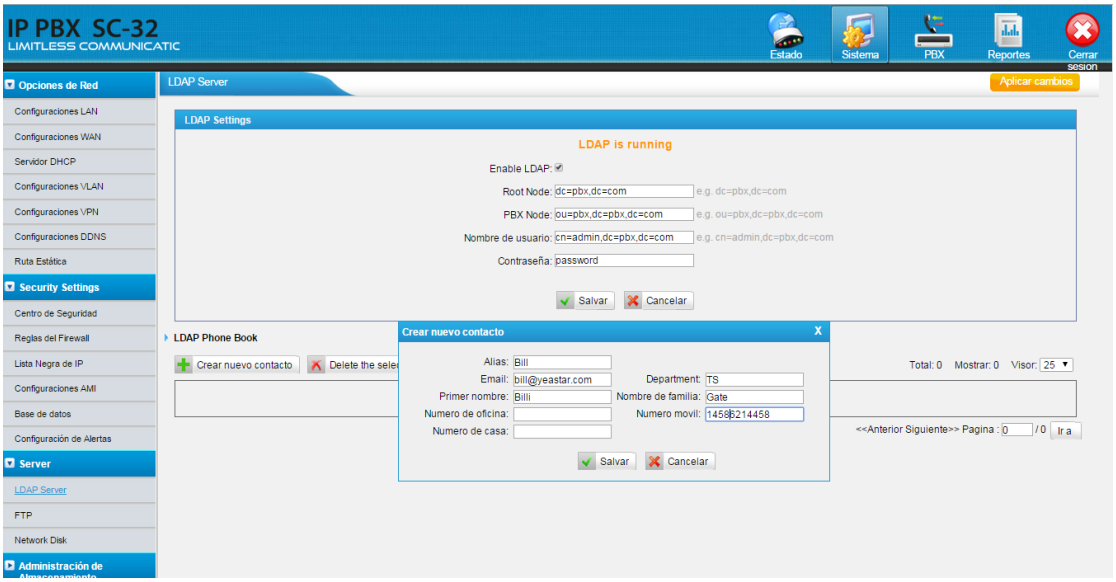


Figura K-1

2. Configuración en teléfono IP Yealink T-28

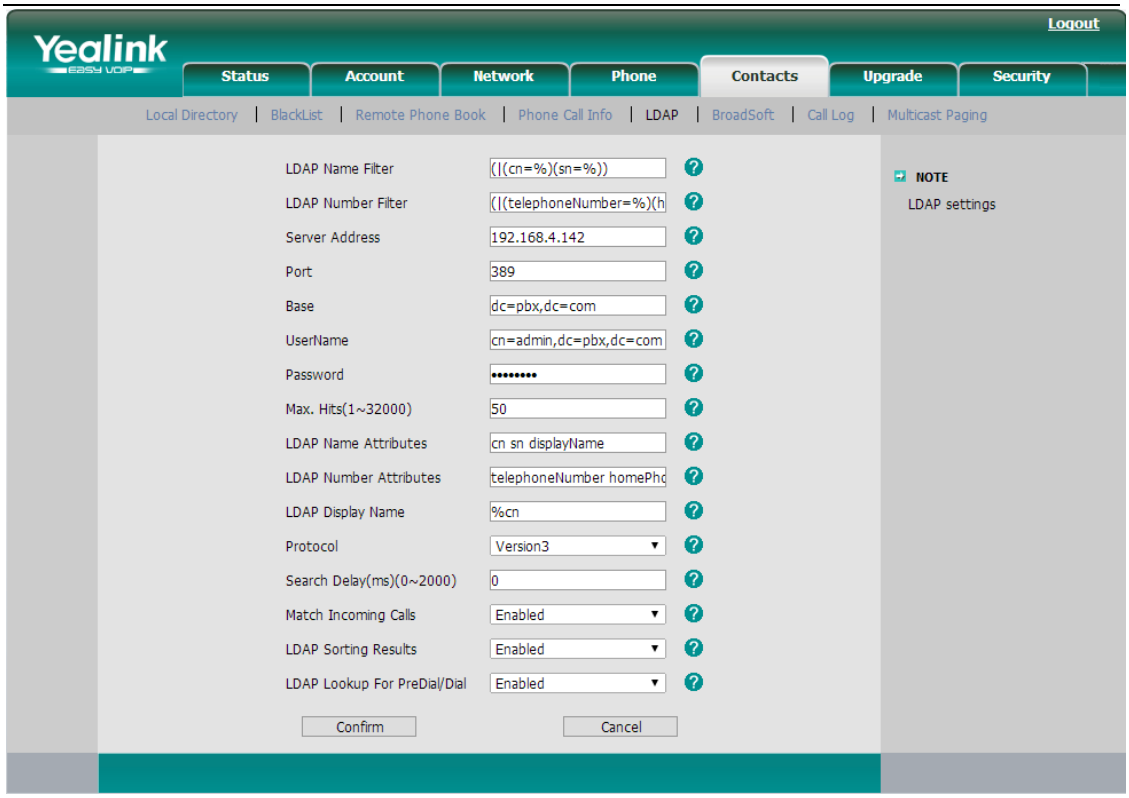


Figura K-2

Primero rellena los campos como las configuraciones de abajo.

Nombre de LDAP Filtro: (|(cn=%)(sn=%))
Número de LDAP Filtro: (|(telephoneNumber=%)(homePhone=%)(mobile=%))
Dirección del Servidor: 192.168.5.142 /IP de UNI-K/
Puerto: 389
Base: dc= SISTEK,dc=cn
Nombre del Usuario: cn=admin,dc=SISTEK,dc=com
Contraseña: ****** /la contraseña que establecida en UNI-K/
Max.Hits: 50
Nombre de LDAP Atributos: cn sn displayName
Número de LDAP Atributos: telephoneNumber homePhone mobile mail departmentNumber
Nombre Mostrado LDAP: %cn
Protocolo: Versión 3
Busca demora(ms)(0~2000): 0
Búsqueda LDAP para llamada entrante: Activado
Resultados de clasificación de LDAP: Activado
Búsqueda LDAP para Pre marca/Marca: Activado

Haga clic en el botón "confirmar", y el LDAP llevará a efecto.

Configure la tecla DSS para vincular a la configuración de LDAP.

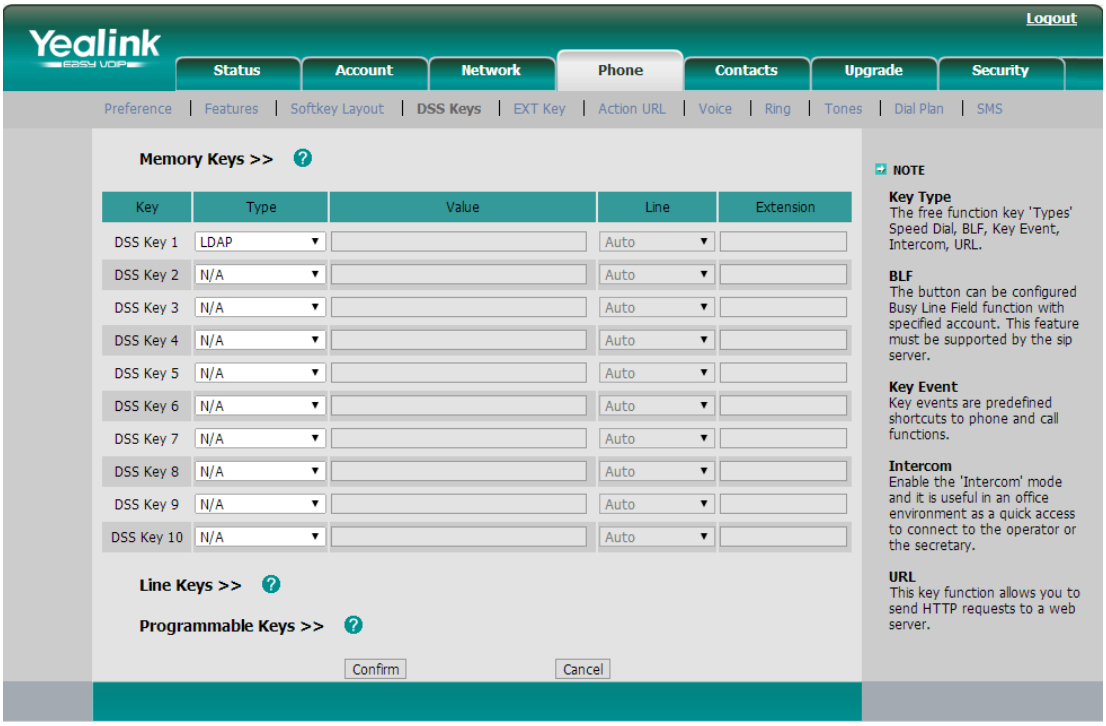


Figura K-3

Si activa la "Búsqueda de LDAP para Pre Marca/Marca", puede utilizar función LDAP en página Pre Marca/Marca o pulsando la tecla de DSS.

[Final]